KETS - District Operations Guide

Windows Server 2008 Domain Services and Outlook Live

Kentucky Department of Education

10/18/12

Version 3.9

EVERY CHILD

PROFICIENT & PREPARED FOR SUCCESS

KENTUCKY DEPARTMENT OF EDUCATION

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change reference
4/30/09	Jeremy Miller	v0.1	Document Creation
9/8/09	John Logan	v0.3	Redesign and build
9/9/09	John Logan	v0.4	Met with Marty/Richard and need to do some work to get the foundation built.
9/10/09	John Logan	v0.5	Adding more Outlook Live info (DLAdmin, permissioning, etc)
9/11/09	John Logan	v0.6	After giving v0.5 to MADS for review. Continuing to add info (mostly Student Admin stuff for Outlook Live)
9/14/09	John Logan	v0.7	Need to save a new copy just in case.. Modified quite a bit in v0.6, and continuing on with DG administration
9/17/09	John Logan	v1.0	Formatting. Sent out on 9/17 to reviewers listed below
9/18/09	John Logan	v1.1	Modified Group Policy Preferences. Started with edits from reviewers
9/21/09	John Logan	v2.0	Working on final version for dispersing to pilots. Applying Richard's edits.
9/22/09	John Logan	v2.1	Post-pilot release modifications. Removed mail2 to point to outlook.com for outages. Also discussed if district have used less than 6 characters and impact during outage. Edited Terminology section. MSI installer update.
1/05/10	John Logan	v2.2	Review after holidays. Read through from beginning to end and made cosmetic changes.
3/26/10	John Logan	V2.3	Update after Richard and Joel's initial review. A thorough review is pending Added KySTE Conference items to the 'to do' list Re-read w/ modifications to prepare for final reengagement
3/30/10	John Logan	V2.4	Everyone reviewed together. Thorough update to R4 4/6 – Went through final run with team
4/8/10	John Logan	V2.5	Pending edits.. Added PowerShell example
4/12/10	John Logan	V2.6	Added Mac/Jeremy's initial edits (to pg 40)
4/12/10	John Logan	V2.7	Added how to reattach deleted user object to mailbox (Tombstoning) PILOT Version
4/14/10	John Logan	V2.8	Added defaults for Tombstoning fn.ln.district@staff.kyschools.us explanation renamed MSI Default instead of MailOnly Moving a user from Staff to Student requires a usertype change

4/28/10	John Logan	V2.9	Reworded how to manually run provisioning (under ‘Jobs’ of KETS Control Panel) Reworded credentials overview under ‘Need to Know’ items Added valid/invalid password characters Client limits in Section 2.9
5/3/10	John Logan	V3.0	Version sent to all districts prior to mass deployment (post-Pilot). Updated Support section with Matt’s modifications Final update of Support Section (5/10)
5/12/10	John Logan	V3.1	Added -32 switch on ADUC for Attribute Editor SPAM and Notifications Update changes to KETS Control Panel Copy posted 2 days prior to migration
6/16/10	John Logan	V3.2	Changed OutlookAdmins to refer to is as a Security Group instead of DL for clarity Need to add EveryoneDL for staff Use BBC when sending Need to add moderating any DLs that have many members Using ‘CheckNames’ in OWA vs hitting the To button to go to GAL mail.kyschools.us/password.aspx instead of live… AD is authoritative (DL names, etc) ADUC disabled user disables mailbox in Outlook Live Apostrophe (and other invalids) in SMTP Powershell to set Secondary E-mails Powershell to add mailbox permissions Outlook Admin to set OutlookAdmins and Notifications membership Make sure contacts/groups are outlined on when they are provisioned Notifications group gets user DL creates Add invalid characters in SMTP addresses Read-receipts time-zone issue Setting access rights for DGs that require SMTP Relay to 500 to 3000 number of recipients, and also Personal DL membership counts Clarify new user creation after deletion and tombstone.. ReRead and ReWord through document.
6/21/10	John Logan	V3.3	Change OET to KIDS Need to add ‘one-pager’ cheatsheet for them to print out Delete ketsEduPlan to allow for MailOnly if NoMail is already set. You could set to MailOnly. State DL permissions Distirbution Group rename Reworded group expansion and how it counts against daily limits PowerShell – set TimeZone and Language Describe how ECP is the way to create/manage DGs Moved OWA Branding under OWA from Student only section as it applies to Staff as well. Reworded Multi-Mailbox Search and added under PowerShell section, but is NOT working at the moment Add to Transport Rules in PowerShell section Modified DIST Staff User Admins description under ‘Disable Mailbox’ section User object deletions only happen at night Describe ‘Company’ attribute flow Changed the Mailbox Retention language from 15 to 30

			Better defined the Staff provisioning interval (15 minutes for kick off, but could take up to an hour) Perform user creations (especially mass creations) in the afternoon and definitely not on a Monday morning (with password resets happening, etc) Add more on how to create a Contact Reworded User Name Changes Distribution Groups and Contacts do NOT flow to Student Tenant Recreate student accounts before school after deletion at beginning of summer – must set e-mail address District specifies SMTP address for both DGs and SGs in ADUC (No ILM to figure it out) Add setting 'Hidden' or 'NoMail' when deleting AD object if the desire is for the person to be 'gone'. Update to Eviction process to clarify Windows Live ID purge instead of evict Add video link in KETS Control Panel section OWA Branding options Add-MailboxPermissions is NOT working and is an open issue 3,000 max on recipients per day and per message Update to support process
8/27/10	John Logan	V3.4	OutlookAdmin permissions are now reconfigured Add-MailboxPermissions Create Contacts with PowerShell Multi-Mailbox Search is now working Add Service Status page When opening a ticket should state that "district is not a Tenant Admin' Add PowerShell examples for common query tasks Groups in AD that need a DG in Live must be a Universal Group Groups and Contact deletions provision once per week. When deleting an AD account 'may' want to set to 'NoMail' first then delete, or set as hidden before AD deletion.
9/13/10	Jeremy Miller	V3.5	Notifications DG must be updated using Powershell Multi-Mailbox Search does not currently work properly Added PowerShell example for updating DG membership Preventing incremented SMTP addresses documented Dynamic Distribution Groups are now working Updated information for creating Dynamic Distribution Groups
12/7/10	Jeremy Miller	V3.6	Multi-Mailbox Search has been fixed and is verified Staff Multi-Mailbox Search PowerShell example has been updated Added information for reporting SPAM to Microsoft Updated District LIVE@EDU Support Flow Updated District Checklist for LIVE@EDU Support
4/9/12	John Fabry	V3.7	Updated deleted item retention (2.10) Shared Live@edu admin account password recommendation (2.6) Updated SMTP Relay for authentication (2.11) Modified IE session switches (2.10.2)
7/31/12	John Fabry	V3.8	Created new section for resource account naming (3.1.9.2) Updated information on hiding accounts from the GAL (3.1.9.3) Additions for password prompt and Live security questions (2.10.2) Updated FOPE information (3.4) Flipped schedule chart (2.6)
10/18/12	John Fabry	V3.9	Updated links for new education.ky.gov page

Reviewers

Name	Version Reviewed	Version Approved	Date
MADS Team	v1.0 (9/17)	Chris Hornfeldt v1.0	9/18/09
Richard Wakeman	v1.0 (9/17)	v1.0	9/18/09
Mike Dube	v1.0 (9/17)		
Marty Park	v1.0 (9/17)		
KETS Service Desk	v1.0 (9/17)	v1.0	9/18/09

Table of Contents

1 Introduction

1.1 Document Purpose

Welcome to the Microsoft Windows Server 2008 Active Directory and Outlook Live Administrator's Guide. This guide outlines the technologies and steps involved in administering the Kentucky Education Technology System (KETS) Active Directory 2008 environment, specifically as it pertains to electronic mail provisioning. The focus of this guide is to convey the necessary tasks for carrying out the routine operations required to administer your district's Active Directory 2008 system and messaging platform. There are other 'authoritative' resources that this document will continually point to for guidance. District administrators should leverage these additional guidelines, with the understanding that some of the components outlined in these guides may not necessarily pertain to our implementation of the system, as some technologies have been designed specifically for KETS.

The KETS deployment of Microsoft's Windows Server 2008 Domain Services (AD) is not complex, it's simply large. The injection of Outlook Live for messaging and the provisioning components make it somewhat complex at an architectural level but the hope is that it is reasonably administrable from a user management position. Outlook Live is a Microsoft offering for 'mail in the cloud', where the servers exist outside of the KETS network. The initial writing of this document will only encompass electronic mail from Outlook Live, though in the coming months other collaborative features will be added to the offering which may require updates to this document.

The KETS AD and Messaging design has been implemented as seamless as possible to allow districts to continue utilizing tools like Active Directory Users and Computers to also administer users which require mail services. It's important for districts to realize that this is not the norm for most users of Outlook Live services. There have been customizations built for KETS which will be defined throughout this document. In the following sections all 'KETS specific' tasks and how they are to be accomplished are described, meaning those tasks that are designed solely for the KETS system for which no other documentation exists. There are specific discussions which may be duplicated in different areas in this guide as they may logically fall in several areas (ex. How to manage Distribution Groups with Exchange Control Panel may be discussed in the *Distribution Group Administration* section but may also be somewhat discussed in the *Exchange Control Panel* section). This document is *not* intended to cover all required end user tasks.

1.2 Audience

This guide was written and is kept up-to-date for the technical administrators and user managers of Kentucky school districts' directory services and messaging systems.

1.3 Technologies/Terminologies

There are acronyms and technology terms that are used when discussing Active Directory and the messaging system implemented in KETS. The technology field is riddled with these terminologies which can cause great confusion if not thoroughly defined. It's first important to reiterate that technical administrators in this K-12 environment are the audience for this document.

The term '**KETS**' will be referenced throughout this document, referring to all users, and technologies, which utilize enterprise services delivered to the 176 (including KSD and KSB) school districts by **KIDS** (the Office of Knowledge, Information and Data Services) which was formerly the Office of Education Technology, or OET. KIDS is the technology office of the Kentucky Department of Education.

Windows Server 2008 Domain Services (also known as Active Directory) is utilized by KETS. The Active Directory Domain Controllers, the devices which run the service, utilize Windows Server 2008 Hyper-V technology. Microsoft's Windows Server 2008 **Hyper-V** provides virtualization of operating systems and their services. KETS also utilizes Domain Name Services (**DNS**) which resides within Active Directory as well as external to Active Directory on other platforms.

Live@edu is Microsoft's offering to educational entities for several technologies that are 'housed' at Microsoft's datacenters throughout the world. These technologies are accessed over the internet by various clients depending on the technology required. KETS has initially adopted only the e-mail service (**Outlook Live**) of Live@edu which is one of several offerings which reside under the Live@edu 'umbrella'. It's important for districts to understand that any user with a **Windows Live ID** can create/access other services. These optional services have been removed from the menus of the e-mail screens but a user can technically utilize other services (Skydrive, Live Workspaces, etc) if they go through the Microsoft offered websites instead of the KETS specifically built ones (explained in detail in following sections).

Access to e-mail services within Outlook Live is available through full-featured MAPI based e-mail applications such as **Outlook 2007** or through **Outlook Web App** (**OWA** – aka Webmail or KETSMail). **Entourage WSE** is the Macintosh based client offering a MAPI-like experience. **Windows Mobile**, other **ActiveSync** based devices as well as some non-ActiveSync devices (IMAP, etc) can also access Outlook Live, though will have limited functionality.

Our different user types (staff and student) exist in Outlook Live in separate areas which are referred to as **Tenants**. These are actually different Exchange Organizations but for the purpose of this document they can be thought of as different Global Address Lists. There are many management options available for each district's 'Student' Tenant such as 'Closed Campus', Bad Word lists, etc which are configurable through the Exchange Control Panel (discussed later).

Online Provisioning System (OLPS) was coined by members of the KETS AD/EX Migration Product Team upon design of the provisioning system. OLPS is built on **Identity Lifecycle Manger (ILM)** which reads and writes to/from Active Directory and Outlook Live. Components of OLPS perform customized tasks to synchronize objects to the mail system.

Some administrative tasks are performed in web portals that are provided to district administrators. These are the **KETS Control Panel** (customized for our environment) and the **Exchange Control Panel**. The tasks that can be performed in these web interfaces as well as the other technologies discussed in this section will be expanded upon throughout this document. From a high-level there are some very specific tasks that can be accomplished through the KETS Control Panel, but there is nothing that is *required* for normal user management. As far as the Exchange Control Panel, it is only used for

Distribution Group (aka. Distribution List) management for the Staff GAL. There are many options available for Student GAL management through the Exchange Control Panel which are discussed in that section.

Note: The Exchange Control Panel is simply what Microsoft calls the configuration area that is available when the 'Options' button is selected while in OWA/Webmail. It is referred to as Exchange Control Panel (ECP) in this document as other documentation will refer to it as such.

Password Change Notification Service (PCNS) allows for passwords in Active Directory and Outlook Live to be in sync. Since Windows Live IDs will be the same as each user's SMTP address OLPS populates the User Principal Name (**UPN**) with the user's primary SMTP address, allowing users to have the login name be the same between AD and Outlook Live if the district user so chooses to utilize UPN. They can always use *domain/user* if desired for login. Because of the password synchronization technology users have the functionality of **Single Sign-On (SSO)** with OWA (https://mail.kyschools.us) and **Same Sign-On** with Outlook 2007 (or Outlook 2010). Single Sign-On provides a 'pass through' experience, which does not require an additional login other than the user's domain login to the computer. Same Sign-On means the username and password are the same, but Outlook will require an additional login.

PowerShell 2.0 is a command-line based scripting language that can be used to administer objects in Outlook Live. There are many functions that can be accomplished only with PowerShell (especially the Staff Tenant). These range from Multi-Mailbox searches to adding secondary proxy addresses to mailboxes.

Again, these technologies and terms will be explained in more detail in later sections.

1.4 Document Feedback

If you have ideas for improving this document, such as adding additional information or clarifying existing content, please send them to your KETS Engineer so they can be considered for future versions.

1.5 Document Updates/Location

This document will be updated and enhanced over time. Please check for new versions periodically at http://education.ky.gov/districts/tech/Pages/Administration-and-Install-Guides.aspx

Note: Please take a moment to visit the areas under http://education.ky.gov/districts/tech/tss/Pages/Outlook-Live-Email-and-KETS-Directory-Services.aspx as there are many valuable instructional tools available that can assist with your administration of these systems.

2 'Need to Know' Items

This section will outline the items that are not necessarily 'task' oriented but are extremely important to the administration of the system. Some of these discussions are expanded upon in Section 3. Please read and understand all of the items that follow as they will serve as the foundation of the Active Directory and Outlook Live systems.

At a high-level there are four major management avenues that can be utilized by an IT admin for AD and messaging administration. These areas are:

1. Active Directory management tools
   - **a.** Active Directory Users and Computers
   - **b.** CSVDE, LDIFDE, etc
   - **c.** DSADD, DSMOD, etc
   - **d.** Other 3rd party tools (AD Infinitum, etc.)
2. KETS Control Panel
3. Exchange Control Panel
4. PowerShell / Exchange Web Services (EWS)

The first two areas (AD tools and KETS Control Panel) are leveraged with those Active Directory credentials that were used in the past that have membership in privileged Security Groups such as DIST Support Admins, DIST Staff User Admins, etc. The third area (Exchange Control Panel) is used specifically for management of the messaging infrastructure. **To summarize, you will login with your administrative Active Directory credentials to do AD and KETS Control Panel tasks**. **Anything in Exchange Control Panel will be a Windows Live ID that does not exist in Active Directory.** These accounts are explained in following sections.

Exchange Control Panel is primarily used for Distribution Group (aka Distribution List) creation and management for Staff users. For students, Exchange Control Panel has other student specific settings. PowerShell and EWS scripted applications also can be leveraged to administer Outlook Live (and AD for that matter). So **you will use 'Outlook Live' administrative accounts that do not exist in Active Directory to perform tasks against Outlook Live (Exchange Control Panel, PowerShell or scripting to the mail system)**.

All administrative credentials are outlined below in the section entitled *Administrative Accounts for Outlook Live and AD*. More management tasks using these credentials are described throughout in Section 3 of this document.

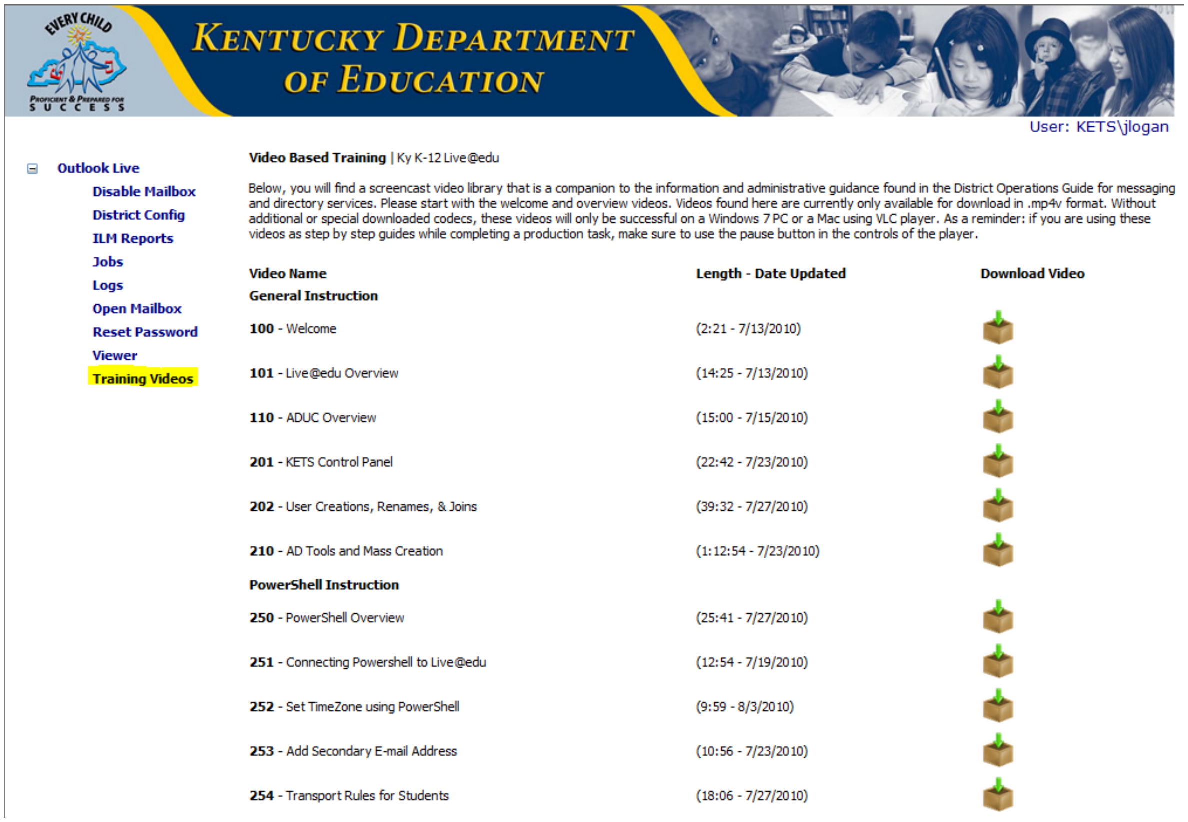
2.1 Active Directory

The KETS Active Directory (AD) environment is built on Windows Server 2008 Domain Services. Active Directory is responsible for user authentication and authorization throughout many services within the district environment. Users rely on DNS within AD as well as 'external' DNS when required. AD is also responsible for DHCP as well as other services.

The design of Active Directory for KETS exists as a classic hub-and-spoke topology, consisting of an 'empty' root domain (KETSDS.NET) with 179 sub-domains. AD replication is linear from each district domain to the hub-site, replicating on a one-hour interval. Each district domain has two AD Domain Controllers which reside physically within the district on KIDS managed hardware. Each district also has an additional AD Domain Controller which resides at KIDS. These tertiary AD Domain Controllers exist in an environment that is called 'DR AD' (Disaster Recovery Active Directory). This environment also contains portions of the OLPS system. Backups of the 'local' domain controllers as well as the offsite DR AD are performed by KIDS.

2.2 KETS Live@edu Videos, Help.Outlook.com and other resources

There are 'accompanying' videos to this guide that can be found on the KETS Control Panel (http://live.kyschools.us/admin/videos.aspx) which may be beneficial to review as a companion to this document. These are provided as a link from the main KETS Control Panel page as well.



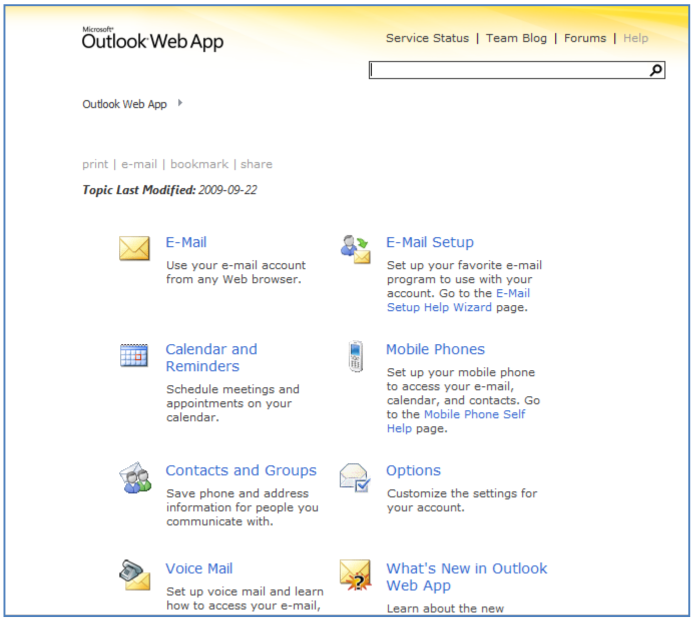
Video Based Training | Ky K-12 Live@edu

Below, you will find a screencast video library that is a companion to the information and administrative guidance found in the District Operations Guide for messaging and directory services. Please start with the welcome and overview videos. Videos found here are currently only available for download in .mp4v format. Without additional or special downloaded codecs, these videos will only be successful on a Windows 7 PC or a Mac using VLC player. As a reminder: if you are using these videos as step by step guides while completing a production task, make sure to use the pause button in the controls of the player.

Video Name	Length - Date Updated	Download Video
General Instruction		
100 - Welcome	(2:21 - 7/13/2010)	⬇
101 - Live@edu Overview	(14:25 - 7/13/2010)	⬇
110 - ADUC Overview	(15:00 - 7/15/2010)	⬇
201 - KETS Control Panel	(22:42 - 7/23/2010)	⬇
202 - User Creations, Renames, & Joins	(39:32 - 7/27/2010)	⬇
210 - AD Tools and Mass Creation	(1:12:54 - 7/23/2010)	⬇
PowerShell Instruction		
250 - PowerShell Overview	(25:41 - 7/27/2010)	⬇
251 - Connecting Powershell to Live@edu	(12:54 - 7/19/2010)	⬇
252 - Set TimeZone using PowerShell	(9:59 - 8/3/2010)	⬇
253 - Add Secondary E-mail Address	(10:56 - 7/23/2010)	⬇
254 - Transport Rules for Students	(18:06 - 7/27/2010)	⬇

http://help.outlook.com can prove to be an administrator's (and end user's) most valuable resource when searching for guidance on common tasks associated with Outlook Live. This site is referenced many times throughout this guide as there is no feasible way to expound on all required tasks that an administrator or user will need to accomplish. The information on the site is always up-to-date and easy to find.

You can traverse through the common tasks or search for more specific information (screen shot below).



Microsoft Outlook Web App

Service Status | Team Blog | Forums | Help

Outlook Web App

print | e-mail | bookmark | share

Topic Last Modified: *2009-09-22*

E-Mail
Use your e-mail account from any Web browser.

E-Mail Setup
Set up your favorite e-mail program to use with your account. Go to the E-Mail Setup Help Wizard page.

Calendar and Reminders
Schedule meetings and appointments on your calendar.

Mobile Phones
Set up your mobile phone to access your e-mail, calendar, and contacts. Go to the Mobile Phone Self Help page.

Contacts and Groups
Save phone and address information for people you communicate with.

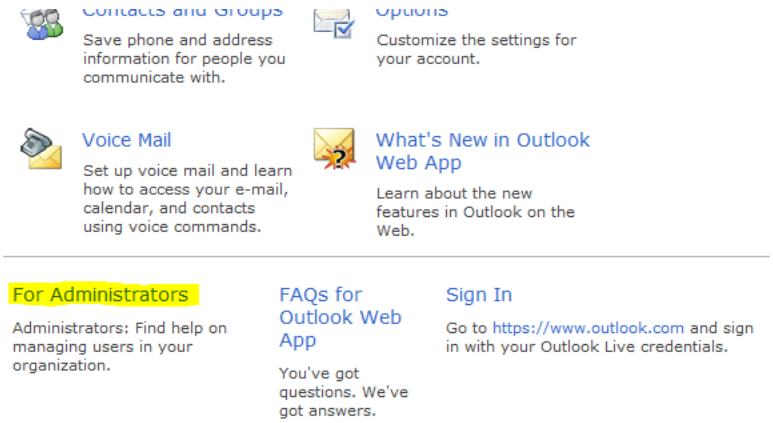
Options
Customize the settings for your account.

Voice Mail
Set up voice mail and learn how to access your e-mail,

What's New in Outlook Web App
Learn about the new

Example: Suppose while in OWA you'd like to open another mailbox that you have access to. To find out to perform this task you would go to http://help.outlook.com and search for 'Access'. This results several links to documents discussing 'Access', one of which is specific to accessing another mailbox.

You may also choose to simply traverse the site by going to the bottom of the help.outlook.com homepage and selecting 'For Administrators' as shown below.



Contacts and Groups
Save phone and address information for people you communicate with.

Options
Customize the settings for your account.

Voice Mail
Set up voice mail and learn how to access your e-mail, calendar, and contacts using voice commands.

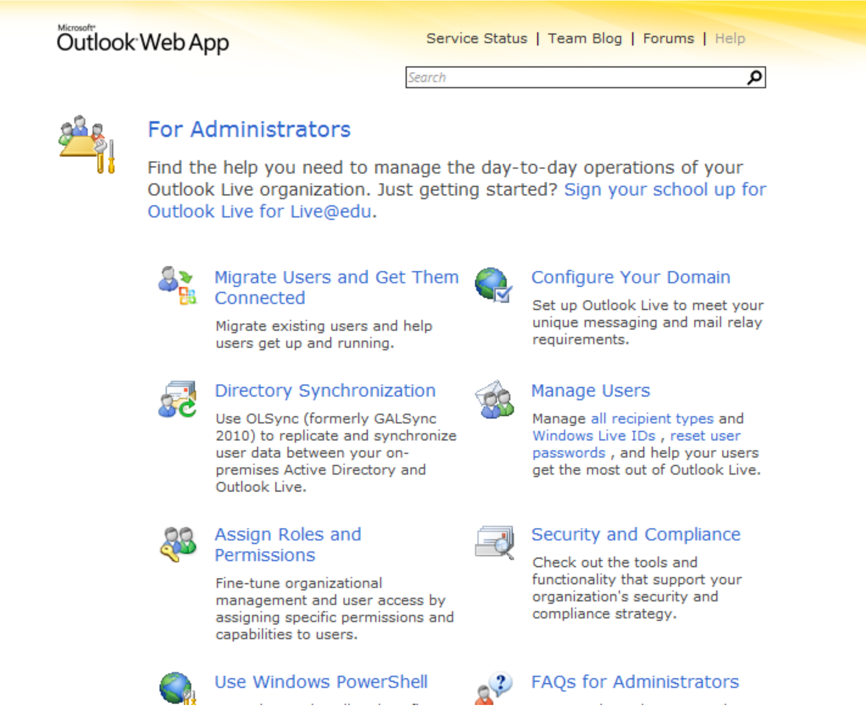
What's New in Outlook Web App
Learn about the new features in Outlook on the Web.

For Administrators
Administrators: Find help on managing users in your organization.

FAQs for Outlook Web App
You've got questions. We've got answers.

Sign In
Go to https://www.outlook.com and sign in with your Outlook Live credentials.

As shown below there are several administrative categories to research


Microsoft Outlook Web App
Service Status | Team Blog | Forums | Help
Search

For Administrators

Find the help you need to manage the day-to-day operations of your Outlook Live organization. Just getting started? Sign your school up for Outlook Live for Live@edu.

Migrate Users and Get Them Connected

Migrate existing users and help users get up and running.

Configure Your Domain

Set up Outlook Live to meet your unique messaging and mail relay requirements.

Directory Synchronization

Use OLSync (formerly GALSync 2010) to replicate and synchronize user data between your on-premises Active Directory and Outlook Live.

Manage Users

Manage all recipient types and Windows Live IDs , reset user passwords , and help your users get the most out of Outlook Live.

Assign Roles and Permissions

Fine-tune organizational management and user access by assigning specific permissions and capabilities to users.

Security and Compliance

Check out the tools and functionality that support your organization's security and compliance strategy.

Use Windows PowerShell

FAQs for Administrators

Note: Some of this information is not applicable as we have had to implement certain provisions in our system to meet various business requirements. The confines to which were implemented are documented throughout this document. That is why the information in this document must be looked at as a prerequisite before implementing instructions found outside of this operation guide.

Information on tasks such as setting the mailbox permissions to open a mailbox, how to share calendars, how to create Resource Calendars, as well as many such tasks can all be found by traversing or searching http://help.outlook.com. This should be used by administrators as well as end users. The information there is more up-to-date and easier to search than if it were duplicated in this guide. It is important to note that some of the search results are actual Q/A by other users, not just 'whitepaper' docs. These can be beneficial in getting answers as well but be aware that these may not be 'official' answers. Also note that the way to perform these desired tasks may be documented on help.outlook.com or other sites but the accounts that you need to use when implementing are discussed in this document.

There are also many publications which define the feature sets and administrative tasks associated with Windows Server 2008 Active Directory services and Microsoft's Live@edu (Outlook Live). Districts should take advantage of these resources. In our environment the most accurate and up-to-date information for Windows Server 2008 Active Directory services as well as Outlook Live can be found on the web at these resources (as well as other publications). Again, a prerequisite should *always* be to reference this document first as there are many customized elements configured specifically for our environment. If the guidance you seek is not in this document then proceed to these other resources for expert guidance, making sure those suggestions 'fit in' with our customized system as outlined in this document.

Examples of web-available resources:

- http://help.outlook.com – Searchable How-To center for Outlook Live
- http://outlookliveanswers.com - Microsoft technical community devoted to Outlook Live
- https://my.liveatedu.com – Your central location for managing the Student Tenant (GAL) for Outlook Live
- https://eduadmin.live.com/Support.aspx - Support center for Outlook Live
- http://technet.microsoft.com – Microsoft resources for IT Professionals
- http://www.microsoft.com/communities/default.mspx - Microsoft technical communities provide opportunities to interact with Microsoft employees, experts, and your peers in order to share knowledge and news about Microsoft products and related technologies

2.3 Support

In general, the KETS Active Directory 2008 and Outlook Live environment works as described in vendor documentation and Help screens. However, some operations have been customized for the KETS environment and must be carried out as described in this document or in consultation with KIDS. If you are not sure whether vendor documentation is correct, Microsoft or otherwise, for a particular task please contact the KETS Service Desk.

For assistance with Active Directory issues, mailbox creation/provisioning errors or KETS Control Panel items please contact the KETS Service Desk. For issues with any Live@edu service (access to Outlook.com, Exchange Control Panel, help.outlook.com, etc) use the information in the following section.

2.4 Windows Live@edu Support Services

Purpose

The purpose of this section is to provide KY Department of Education (KDE) Office of Knowledge & Information Services (KIDS) support staff guidance on how to properly obtain support on Live@EDU related support issues. This is a guide only and does not and cannot address every possible scenario. Where content exists in another source that document is referenced.

Questions/comments related to the content in this document should be directed to the Technical Account Manager.

Terms

KIDS: Knowledge & Information Data Services (formerly the Office of Education Technology (OET))
Premier: Microsoft Premier Support organization for the Live@edu system.
OLPS: Outlook Live Provisioning System – Maintained by KIDS
DOG: District Operations Guide.

SSO: Single Sign On

Triage Process

Live@EDU is designed in such a way that initial triage and problem resolution should be handled at the level closest to the end-user. In the case of KDE this should be at the District IT level. District IT staff should be fully encouraged to not adopt a "quick trigger" on escalations to Premier Support or KIDS. The following information is meant to aid the District IT staff in triaging Live@EDU issues and Figure 1 provides a flow of the overall process. District IT should follow this guidance to ensure issues are properly examined and attempts are made to resolve prior to escalation.

2.4.1 District-level troubleshooting, before calling KETS Service Desk

NOTE: Completing all applicable troubleshooting notes below can greatly decrease the time to resolve LIVE@EDU issues that may arise.

- □ Ensure AD account is created in an appropriate OU and is not stamped with NOMAIL on the KETS EDU tab.
- □ Ensure enough time has elapsed for the account to be provisioned. Typically provisioning can take up to 2 hours for staff and 6 hours for students.

- ☐ Review the Active Directory object for potential issues
- ☐ Access the “Viewer” section of the KETS Control Panel and ensure that all checkboxes are green. Review any red “X’s” to help determine the problem.
- ☐ Review the “Logs” section of the KETS Control Panel for errors on the account.
- ☐ Ensure that a password reset has occurred for the user, if this is a new or rarely used account.
- ☐ Review the related account in the Exchange Control Panel for potential issues.
- ☐ Can the account be accessed using the KETS SSO page?
- ☐ Can the account be accessed using Outlook.com? (*NOTE: Password reset may not have occurred if the account can be accessed via SSO and not directly from Outlook.com.*)
- ☐ If the issue is related to use of the web pages of Outlook Live then contact Microsoft Premier Support (i.e. Outlook Web App and the Exchange Control Panel).
- ☐ Use the Microsoft Office Outlook Connectivity Test to determine if this is a local network issue.

<u>The following should be provided when opening a ticket with the KETS Service Desk:</u>

- ☐ Detailed description of the problem, including any specific symptoms experienced
- ☐ Example account(s) that are currently experiencing the issue. If multiple users are experiencing this issue, be prepared to provide at least a few examples.
- ☐ Any errors that were noted on the account in the KETS Control Panel Logs or Viewer
- ☐ Detailed description of any troubleshooting that has been performed at the district level
- ☐ Frequency of the problem; intermittent or 100% of the time.
- ☐ Is the problem currently occurring? If not, when was the last occurrence?

Case Workflow

Figure 1 details the case workflow that should be used.

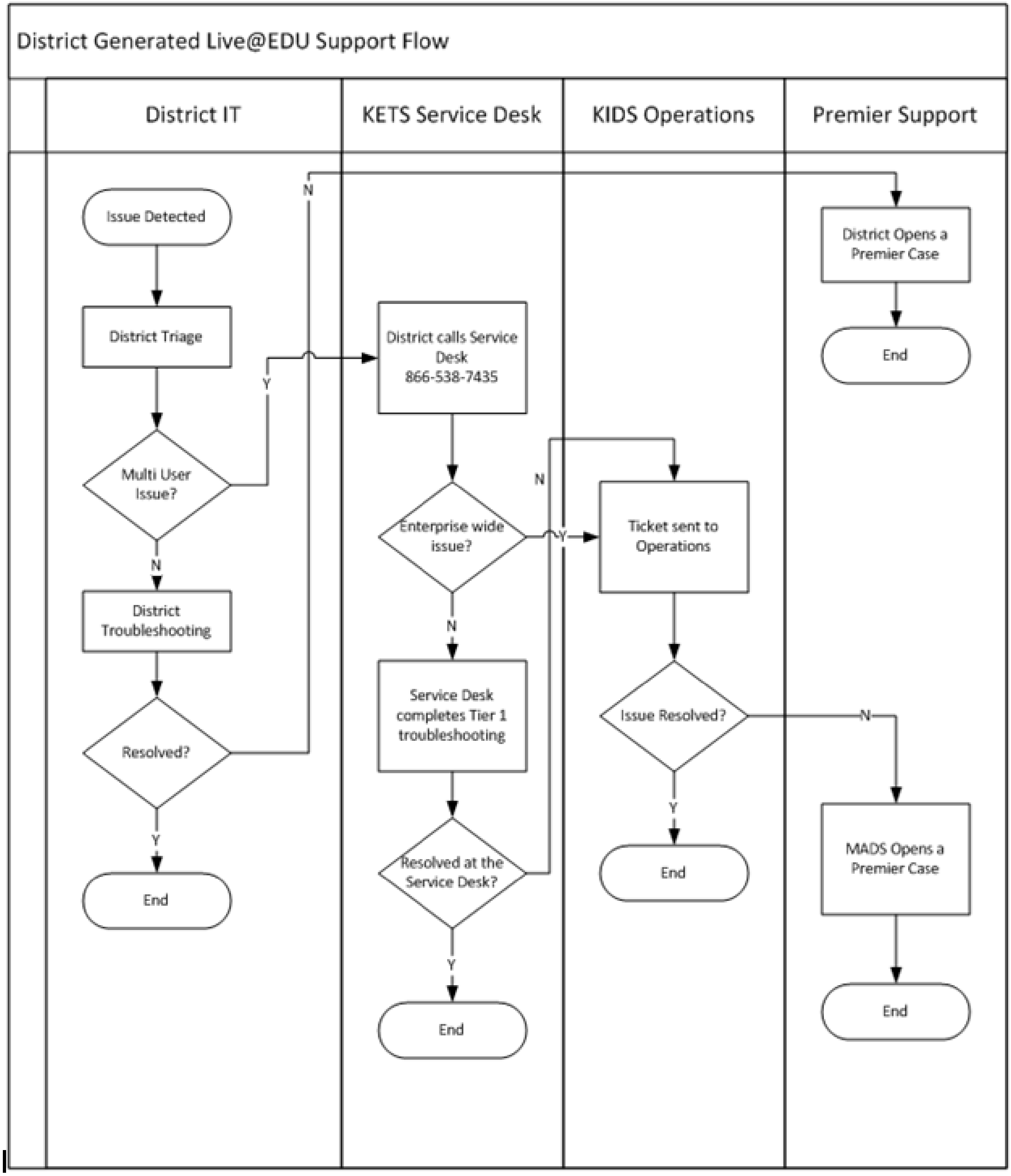

District Generated Live@EDU Support Flow
District IT
KETS Service Desk
KIDS Operations
Premier Support
Issue Detected
District Triage
Multi User Issue?
Y
N
District Troubleshooting
Resolved?
Y
N
End
District calls Service Desk 866-538-7435
Enterprise wide issue?
Y
N
Service Desk completes Tier 1 troubleshooting
Resolved at the Service Desk?
Y
N
End
Ticket sent to Operations
Issue Resolved?
Y
N
End
District Opens a Premier Case
End
MADS Opens a Premier Case
End

Figure 1

2.4.2 Contacting Premier Support

Technical support to address questions or resolve issues you may experience related to Live@edu service is available to you 24 hours a day, 7 days a week via phone or web (KIDS Only). Examples of issues technical support can assist you with include difficulty with the Live ID issues, Outlook Live delays, content migration, students cannot log in, etc.

Phone Support: (800) 936-3100
Web Support: https://premier.microsoft.com

Support entitlement/authentication for access to support is by Access ID. District Technology coordinators should contact their KE to receive their appropriate Access ID. When working with a support engineer during troubleshooting you may need to tell them you do not have 'Tenant Admin' privileges. If the support engineer needs you to perform certain tasks which you do not have access to do you will need to contact the KETS Service Desk to escalate those procedures.

******NOTE******

Districts with their own Premier Support Agreements should use the Access IDs they already have.

Access ID should be kept PRIVATE and CONFIDENTIAL with a very limited number of people in a district. Reporting is keyed off this Access ID and it is critical that districts protect the integrity of their Access ID.

******NOTE******

District IT Support requests submitted for products other than Windows Live@EDU will be closed. Currently there is not a programmatic method to prevent cases from getting opened for non- Windows Live@EDU products. ***ANY DISTRICT THAT OPENS A PREMIER CALL FOR A PRODUCT OTHER THAN LIVE@EDU MAY BE SUBJECT TO FINANCIAL CHARGES APPLIED BY MICROSOFT***

Please refer all single user issues that involve MSN and Windows Live services to http://support.live.com.

For district opened cases that experience a service delivery issue, the district IT staff should contact KIDS via the KETS Service Desk. A representative from KIDS will contact the Technical Account Manager for escalation support. For KIDS and districts with Premier Support, contact the Technical Account Manager for escalation support.

2.4.3 KETS Service Desk Support

For assistance with the following issues, please contact the KETS Service Desk:
- Active Directory issues
- Mailbox creation/provisioning errors
- KETS Control Panel issues
- If you're not sure whether vendor documentation is correct, Microsoft or otherwise, for a particular task

KETS Service Desk:
(502) 564-2002 (local) (866) 538-7435 (toll free)

E-mail: ketshelp@education.ky.gov
Web Support Form
Remedy Mid-Tier System

Additional Web Resources for Live@edu end users:
http://help.outlook.com – Searchable How-To center for Outlook Live Page 20 KETS – District Operations Guide for Active Directory and Messaging Services
http://outlookliveanswers.com - Microsoft technical community devoted to Outlook Live
https://eduadmin.live.com/Support.aspx - Support center for Outlook Live
http://www.microsoft.com/communities/default.mspx - Microsoft technical communities provide opportunities to interact with Microsoft employees, experts, and your peers in order to share knowledge and news about Microsoft products and related technologies

Additional web resources for administrators:
http://technet.microsoft.com – Microsoft resources for IT Professionals
https://my.liveatedu.com – Your central location for managing the Student Tenant (GAL) for Outlook Live

2.4.4 Common Issues

This section provides a list of typical general issues that have been seen during Live@EDU deployments. KDE's deployment of Live@EDU is unique and has the potential for issues that have not experienced in past deployments.

Client Configuration
These often can appear as connectivity issues depending on the client's configuration regarding the display of task bar alerts. Client configuration is detailed in the DOG. This should be resolved by District IT.

Mail being sent to junk email folder
Vast majority of these issues are directly tied to IP Safe-listing issues. End users typically don't check the folder by default and the behavior on Outlook Live may be different than expected (mail from recipients previously not marked as junk now being marked as junk). This should be resolved by District IT.

First time login/password replication issues
This usually related to real-time provisioned customers seeing PCNS delays with password replication. Not sure if this is applicable to KDE. This will typically resolve itself but if not after 30 minutes, the issue should be resolved by District IT.

Forwarding
Mail forwarding rules may not function as expected. Checking junk mail at the endpoint mailbox usually finds the email in a junk folder; junk mail does not get forwarded. This should be resolved by District IT.

Account / Mailbox Provisioning
Account and mailbox creation are typically evident when a client cannot connect to a mailbox or a user cannot login to the service. This can be readily investigated by District IT and, if the account appears good and the mailbox has been provisioned, should be escalated to KIDS.

2.5 GAL Visibility

The KETS implementation into Outlook Live consists of a single Staff Tenant and individual district Student Tenants. A Tenant is similar to an Exchange Global Address List (or Active Directory Forest) for the purposes of this discussion. There are sections throughout this guide which expand on the following discussion points. The following is a high-level summary of Global Address Lists.

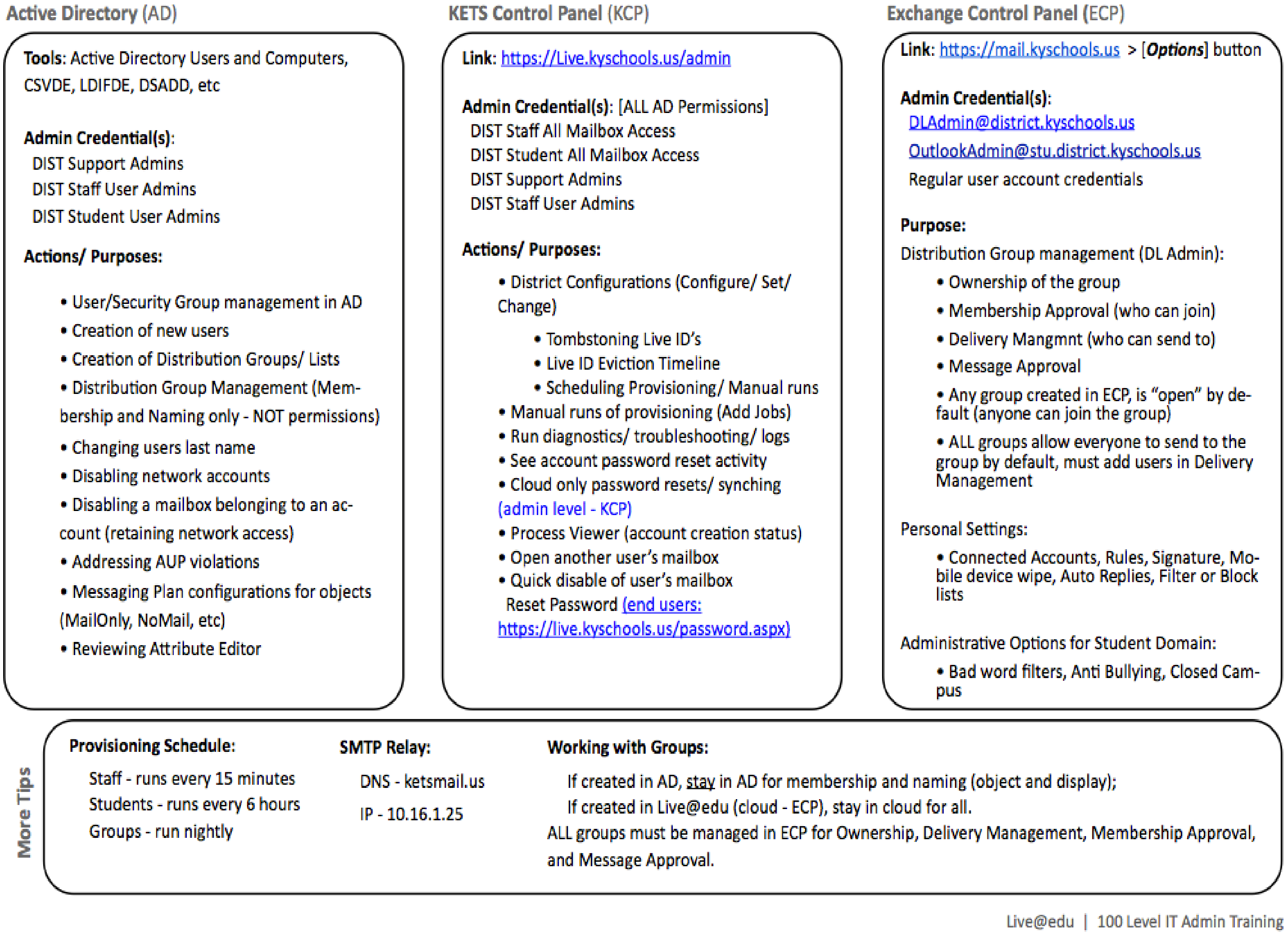
There is one State-wide shared Global Address List (tenant) for staff, available to and containing all district/KDE staff in the state (including all other State Agency staff). There are no other Global Address Lists or Address Lists for staff, meaning there is no segregation of 'district only' objects. Any mailbox or Distribution Group that is assigned as 'Staff' will be seen by all staff in the KETS system. There will be no students visible in the Staff GAL, not even a given district's students. Districts can create contacts for the students in the Staff Tenant/GAL if they wish but those student contacts will be seen by all staff in the KETS system.

The students will not see any objects in their Global Address List other than their own mailbox and the DLAdmin mailbox. Students will not show as members in any Global Address List, staff or student. A district's Student Tenant (GAL) will allow for district administration (through Remote PowerShell, etc) for only those students within the district. Because of the business requirement of an 'All Staff' Global Address List, all staff members exist in one 'Tenant'. Permission cannot be granted for certain tasks to only run against a given district's users, meaning there are some 'top-level' permissions that grant access to the entire 'Tenant' (Staff Tenant in this discussion), which would allow someone to administer all staff objects in the state. In other words there are tasks that are available for each district's Student Tenant that will not be available for Staff. By way of example, in the student tenant a district admin may use PowerShell to set passwords on mailboxes; however, in the staff tenant, the authority to reset passwords through PowerShell is state-wide and has been disallowed for individual district admins. The alternative, for this specific example, is to use the KETS Control Panel (https://live.kyschools.us/admin) to perform the password reset operation, or Active Directory Users and Computers as it is authoritative and will 'sync' to Outlook Live.

2.6 Administrative Accounts for Outlook Live and AD

These administrative accounts are discussed in detail throughout the document in their respective areas. However, it was thought helpful to discuss them collectively in a summarized format. The following is a list of Security Groups in AD which are utilized within the Outlook Live system, as well as 'elevated' accounts/groups which exist in Outlook Live. *Note:* There are other groups in Active Directory (ex. *DIST Staff Account Reset)* which allow user password resets within AD which ultimately flow to the Windows Live ID, but are not discussed here. Below is a 'one-pager' that districts can refer to somewhat as an IT Admin for Live@edu Cheat Sheet.

Below is a brief description of the different Admin accounts for Staff and Student administration. Some are used in ADUC and KETS Control Panel while others are used for direct management in ECP and PowerShell. The differences are noted below.



Active Directory (AD)

Tools: Active Directory Users and Computers, CSVDE, LDIFDE, DSADD, etc

Admin Credential(s):
DIST Support Admins
DIST Staff User Admins
DIST Student User Admins

Actions/ Purposes:

- User/Security Group management in AD
- Creation of new users
- Creation of Distribution Groups/ Lists
- Distribution Group Management (Membership and Naming only - NOT permissions)
- Changing users last name
- Disabling network accounts
- Disabling a mailbox belonging to an account (retaining network access)
- Addressing AUP violations
- Messaging Plan configurations for objects (MailOnly, NoMail, etc)
- Reviewing Attribute Editor

KETS Control Panel (KCP)

Link: https://Live.kyschools.us/admin

Admin Credential(s): [ALL AD Permissions]
DIST Staff All Mailbox Access
DIST Student All Mailbox Access
DIST Support Admins
DIST Staff User Admins

Actions/ Purposes:

- District Configurations (Configure/ Set/ Change)
  - Tombstoning Live ID's
  - Live ID Eviction Timeline
  - Scheduling Provisioning/ Manual runs
- Manual runs of provisioning (Add Jobs)
- Run diagnostics/ troubleshooting/ logs
- See account password reset activity
- Cloud only password resets/ synching (admin level - KCP)
- Process Viewer (account creation status)
- Open another user's mailbox
- Quick disable of user's mailbox

Reset Password (end users: https://live.kyschools.us/password.aspx)

Exchange Control Panel (ECP)

Link: https://mail.kyschools.us > [*Options*] button

Admin Credential(s):
DLAdmin@district.kyschools.us
OutlookAdmin@stu.district.kyschools.us
Regular user account credentials

Purpose:
Distribution Group management (DL Admin):

- Ownership of the group
- Membership Approval (who can join)
- Delivery Mangmnt (who can send to)
- Message Approval
- Any group created in ECP, is "open" by default (anyone can join the group)
- ALL groups allow everyone to send to the group by default, must add users in Delivery Management

Personal Settings:

- Connected Accounts, Rules, Signature, Mobile device wipe, Auto Replies, Filter or Block lists

Administrative Options for Student Domain:

- Bad word filters, Anti Bullying, Closed Campus

More Tips

Provisioning Schedule:
Staff - runs every 15 minutes
Students - runs every 6 hours
Groups - run nightly

SMTP Relay:
DNS - ketsmail.us
IP - 10.16.1.25

Working with Groups:
If created in AD, stay in AD for membership and naming (object and display);
If created in Live@edu (cloud - ECP), stay in cloud for all.
ALL groups must be managed in ECP for Ownership, Delivery Management, Membership Approval, and Message Approval.

Live@edu | 100 Level IT Admin Training

Important: For any of the shared accounts below that exist only in the cloud, it is important to remember that districts with multiple IT personnel will be sharing these accounts. Any time staff changes, you will want to make sure that the passwords to those accounts are changed accordingly. This is especially important since accessing a district's Live@edu information via PowerShell can be done from any computer with an Internet connection; one does not have to be on the district's network to gain access as long as the credentials are known.

Staff

- **OutlookAdmin@*district*.kyschools.us**
  - This is an Outlook Live account (not in Active Directory)

  - MUST access through www.outlook.com, not mail.kyschools.us
  - Used for certain Recipient and Distribution Group administration, such as adding secondary SMTP Proxy addresses to mailboxes.
  - Tasks can only be accomplished with PowerShell 2.0

- **OutlookAdmins@*disctrict*.kyschools.us**
  - This is an Outlook Live Security Group whose members have the same access as the Outlook Admin account (this is not Active Directory)
  - Read-Only ECP access
  - MUST access through www.outlook.com, not mail.kyschools.us
  - ***OutlookAdmin has ownership, not DLAdmin***
  - Limited PowerShell only for certain rights
    - Create new DG &DDG
    - DL/DDG Management
    - Recipient Management

- **DLAdmin@*district*.kyschools.us**
  - This is an Outlook Live account (not in Active Directory)
  - MUST access through www.outlook.com, not mail.kyschools.us
  - Set as 'Owner' of all district Distribution Groups, whether created by Admins or users

- **SearchAdmin@*district*.kyschools.us**
  - This is an Outlook Live account (not in Active Directory)
  - Used for Multi-Mailbox searches across all of a district's staff mailboxes
  - Tasks can only be accomplished with PowerShell 2.0
  - Has access to open **SearchResults_*district*@staff.kyschools.us**, where district is the district SMTP Domain Name.

    Note: Search results are exported to ***SearchResults_****district****@staff.kyschools.us*** *mailbox (notice that the suffix is staff.kyschools.us for all districts)*

- **ServiceAdmin@*district*.kyschools.us**
  - This is an Outlook Live account (not in Active Directory)
  - This is a Service Account only to be used to authenticate applications written to Exchange Web Services.
  - Has 'impersonation rights' to district staff mailboxes.

- **Notifications@*district*.kyschools.us**
  - This is an Outlook Live Distribution Group (not in Active Directory)
  - Members of this group receive OPLS errors for Staff and Students, as well as Staff DG creation notifications
  - Membership must be updated using OutlookAdmin account
  - Membership can only be updated using PowerShell 2.0
  - ***OutlookAdmin has ownership, not DLAdmin***

- Members of the Active Directory group ***<u>DIST Support Admins</u>***
    - Security Group in Active Directory
    - User management access for Staff and Students accounts
    - Management access through Active Directory Users and Computers and KETS Control Panel

- Members of the Active Directory group ***<u>DIST Staff All Mailbox Access</u>***
    - Security Group in Active Directory
    - Access to open Staff user mailboxes
    - Management access through KETS Control Panel

- Members of the Active Directory group ***<u>DIST Staff User Admins</u>***
    - Security Group in Active Directory
    - User management access for Staff (create users, reset passwords, etc)
    - Management access through KETS Control Panel

Students

- **OutlookAdmin@stu.***district***.kyschools.us**
    - This is an Outlook Live account (not in Active Directory)
    - MUST access through www.outlook.com, not mail.kyschools.us
    - Full administrative access to the Student Tenant settings as well as user management
    - Ability to delegate administrative roles to other users
    - Management access through Exchange Control Panel or Remote PowerShell

- **DLAdmin@stu.***district***.kyschools.us**
    - This is an Outlook Live account (not in Active Directory)
    - MUST access through www.outlook.com, not mail.kyschools.us
    - Set as 'Owner' of any Distribution Groups in the Student Tenant (if any are created)
    -

- **SearchAdmin@stu.***district***.kyschools.us**
    - This is an Outlook Live account (not in Active Directory)
    - MUST access through www.outlook.com, not mail.kyschools.us
    - Used for Multi-Mailbox searches across all of a district's student mailboxes
    - Tasks can only be accomplished with PowerShell 2.0
    - Has access to open **SearchResults @stu.***district***.kyschools.us**, where district is the district SMTP Domain Name

      Note: Search results are exported to ***SearchResults@stu.***district***.kyschools.us*** *mailbox*

- **ServiceAdmin@stu.*district*.kyschools.us**
    - This is an Outlook Live account (not in Active Directory)
    - MUST access through www.outlook.com, not mail.kyschools.us
    - This is a Service Account only to be used to authenticate applications written to Exchange Web Services
    - Has 'impersonation rights' to district student mailboxes.

- **Quarantine@stu.*district*.kyschools.us**
    - This is an Outlook Live account (not in Active Directory)
    - MUST access through www.outlook.com, not mail.kyschools.us
    - Used to access 'quarantined' messages by SPAM Filter.
    - **District admins should check this mailbox often, and clean out and forward false-positives to the recipient(s)**

- Members of the Active Directory group ***DIST Support Admins***
    - Security Group in Active Directory
    - User management access for Staff and Students accounts
    - Management access through Active Directory Users and Computers and KETS Control Panel

- Members of the Active Directory group ***DIST Student All Mailbox Access***
    - Security Group in Active Directory
    - Access to open Student user mailboxes
    - Management access through KETS Control Panel

- Members of the Active Directory group ***DIST Student User Admins***
    - Security Group in Active Directory
    - User management access for Students (create users, reset password, etc)
    - Management access through KETS Control Panel

2.7 Responsibilities

2.7.1 KIDS/Microsoft

KIDS is responsible for most technical maintenance and support of systems in the KETS Active Directory 2008 environment. KIDS is also responsible for OLPS which delivers the provisioning between AD and messaging. KIDS is also responsible for SMTP relaying services for secondary applications which require 'send mail' capabilities.

2.7.2 District

Districts are responsible for the physical environment which houses the Active Directory servers. This area should stay physically secure and temperature controlled. The district is also responsible for all user/object administration as well as any licensing that's required.

2.8 Acceptable Use Policy

All districts ***must*** add the following language to Acceptable Use Policies for end user compliance. Federal law requires that any child age 13 and under have parental consent to access online services, such as the Microsoft's Live@edu offering. Of the variety of methods required of any online service provider, Microsoft has chosen – at Kentucky's request – to rely on the respective districts to obtain such consent via the local AUP and accompanying procedures.

> *The Outlook Live e-mail solution is provided to your child by the district as part of the Live@Edu service from Microsoft. By signing this form, you hereby accept and agree that your child's rights to use the Outlook Live e-mail service, and other Live@Edu services as the Kentucky Department of Education may provide over time, are subject to the terms and conditions set forth in district policy/procedure as provided and that the data stored in such Live@Edu services, including the Outlook Live e-mail service, are managed by the district pursuant to policy 08.2323 and accompanying procedures. You also understand that the Windows Live ID provided to your child also can be used to access other electronic services that provide features such as online storage and instant messaging. Use of those Microsoft services is subject to Microsoft's standard consumer terms of use (the Windows Live Service Agreement), and data stored in those systems are managed pursuant to the Windows Live Service Agreement and the Microsoft Online Privacy Statement. Before your child can use those Microsoft services, he/she must accept the Windows Live Service Agreement and, in certain cases, obtain your consent.*

2.9 User Principal Name (UPN) Login– SMTP Login

The User Principal Name attribute, which exists on all user objects in Active Directory, was created for companies that wanted a unique user definition to the login process which isn't bound by domain designs. The UPN attribute in the KETS environment is set by OLPS to be equal to the user's primary SMTP Address (example: *bob.snow@bell.kyschools.us*). All users are encouraged to log in to domain resources using the full KETS user address (UPN, or SMTP). https://outlook.com requires login with the Windows Live ID, which is the SMTP address. Having users log in with their SMTP Address will

> *1)* Give the users one less thing to remember as all users utilizing mail will need to know their e-mail address, but now will not have to know their *domain\user* credentials as well
>
> *2)* Eliminate confusion for users either logging in to outlook.com vs. mail.kyschools.us. Outlook.com requires UPN/SMTP logon, where mail.kyschools.us allows for either UPN or the *domain\user* syntax.

3) Eliminate confusion for Outlook users who will be prompted for e-mail login with the same Windows Live ID.

Note: District users will continue to have the capability to login with domain\user if the district or user so desires.

The user will experience differences in accessing e-mail services depending on which client they use. These differences are explained in the following sections.

2.10 E-mail Client access to Outlook Live

With Outlook Live combined with the Password Change Notification Servers and Single Sign-On functionality within OLPS the user experience is as streamlined as possible, in some ways providing more functionality than Exchange Server installed 'On-Premise'. The areas below discuss different client environments and how they react with Outlook Live.

Note: Configuration within Outlook Live is set for 30 days on deleted items, 14 days on the "dumpster" items retention, for a total of 44 days of content retention. This means that items placed in the Deleted Items folder, through 'deleting' a message, will be purged from the Deleted Items folder 30 days from the message's receive date. Users can still 'Recover Deleted Items' for an additional 14 days after the message is 'purged'. This is a mailbox setting, meaning that this is the case no matter the client being used (Outlook, OWA, etc).

There is a maximum of 3,000 recipients per day a user can send messages to. This is also the maximum number of recipients one can send to on a single message. Public Distribution Groups count as 1 recipient for the entire group, meaning the members are not expanded to calculate the limit. *Personal Distribution Lists each member in the list count as a separate recipient.*

These limits have been raised for KETS, which means you will see it in documentation at Microsoft as 500 recipients per day and 100 recipients per message. **There are many limits outlined at the following link:** http://help.outlook.com/en-us/140/dd630704.aspx

Note: There is a 197 KB limit on the amount of information that can be added to the To: header in OWA, which means that users will get an error in OWA if they add 'too many' recipients, 'too many' many over 197 KB of size which is not very helpful but that's technically how it's built and stated.

2.10.1 Shared Calendars

Users/Admins have the ability to create 'Shared Calendar' which can be accessed by numbers of users. There are two options for deploying these calendars which are listed below.

Create a dedicated user object for the calendar – IT Admins can create an AD object or create a mailbox through Exchange Control Panel. Name this object the name of the desired Calendar and utilize this mailboxes calendar and modify permission.

Secondary User Based Shared Calendars - users can create additional calendars within their account (right click and "Create new calendar") and delegate permissions. The one drawback to this method is if the user object is deleted (person leaves the district) the calendar is lost.

2.10.2 Outlook Web App (OWA) and Single Sign-On (SSO)

There are a couple of ways to access e-mail through a web browser. The primary link to access all Web mail services will be https://mail.kyschools.us. District users also have the ability as well to utilize https://outlook.com, which is the normal public offered link for access to Outlook Live. With this stated districts could have users utilizing the KETS customized page (https://mail.kyschools.us) for primary access and, in the case of an outage of some kind, use https://outlook.com. Districts could either add this second link to a local web page or simply inform the users of both links.

Note: https://mail.kyschools.us will not work if users are using VPN into KDE/KIDS from off-site. If this is the scenario those users should use https://outlook.com

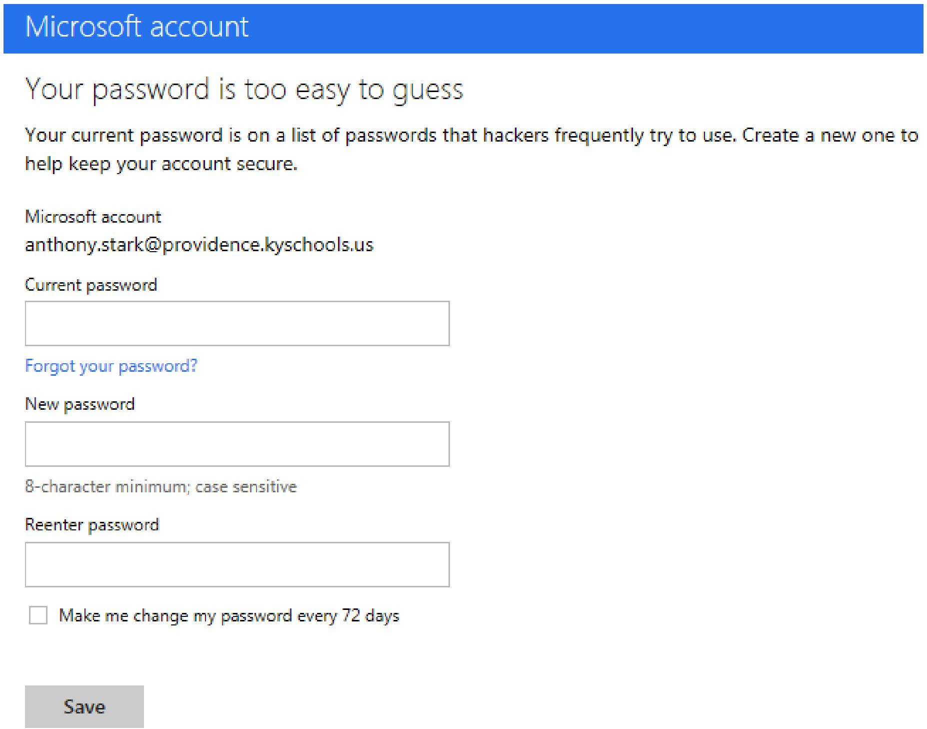
www.outlook.com should be utilized for any 'administrative' tasks that need to be performed in the Exchange Control Panel instead of using mail.kyschools.us. The reason for this is mail.kyschools.us will use the Active Directory credentials of the user logged in to the workstation. For using accounts such as DLAdmin@..., OutlookAdmin@... etc, you will need to login to www.outlook.com as the Windows Live ID of an Outlook Live admin, as they do not exist in Active Directory.

Note: There's a 24 hour timeout for inactivity in OWA which uses the Windows Live ID timeout instead of having one configured. There is no 'Public' option as before which had a few minute timeout.

The KETS link to OWA, https://mail.kyschools.us, provides Single Sign-On (SSO) as well as auditing from Active Directory to Outlook Live. This means that any user who is logged into a KETS Active Directory Domain will be authenticated in with their corresponding Windows Live ID through the web portal. This will happen without user knowledge.

NOTE: *Windows Live IDs require a six character password by default (discussed in section 'Password Complexity Requirements'). District users who utilize https://mail.kyschools.us will **NOT** have to have a six character password in Active Directory, as SSO takes care of this. **HOWEVER**, it's important to note that users who do not have a six character password in AD would not be able to utilize https://outlook.com to access their e-mail, meaning if https://mail.kyschools.us were unavailable due to network issues, etc those users would not be able to access their e-mail. Network issues refer to connectivity between the hub site which hosts OLPS (KDE/KIDS) and the Internet 'cloud'.*

As part of their increased security measures, Microsoft also blocks the use of common passwords that still meet or exceed the minimum password length. For example, if using a password like "123456" or "password" users will likely see the following prompt when looking in to https://outlook.com:



Microsoft account

Your password is too easy to guess

Your current password is on a list of passwords that hackers frequently try to use. Create a new one to help keep your account secure.

Microsoft account
anthony.stark@providence.kyschools.us

Current password

New password

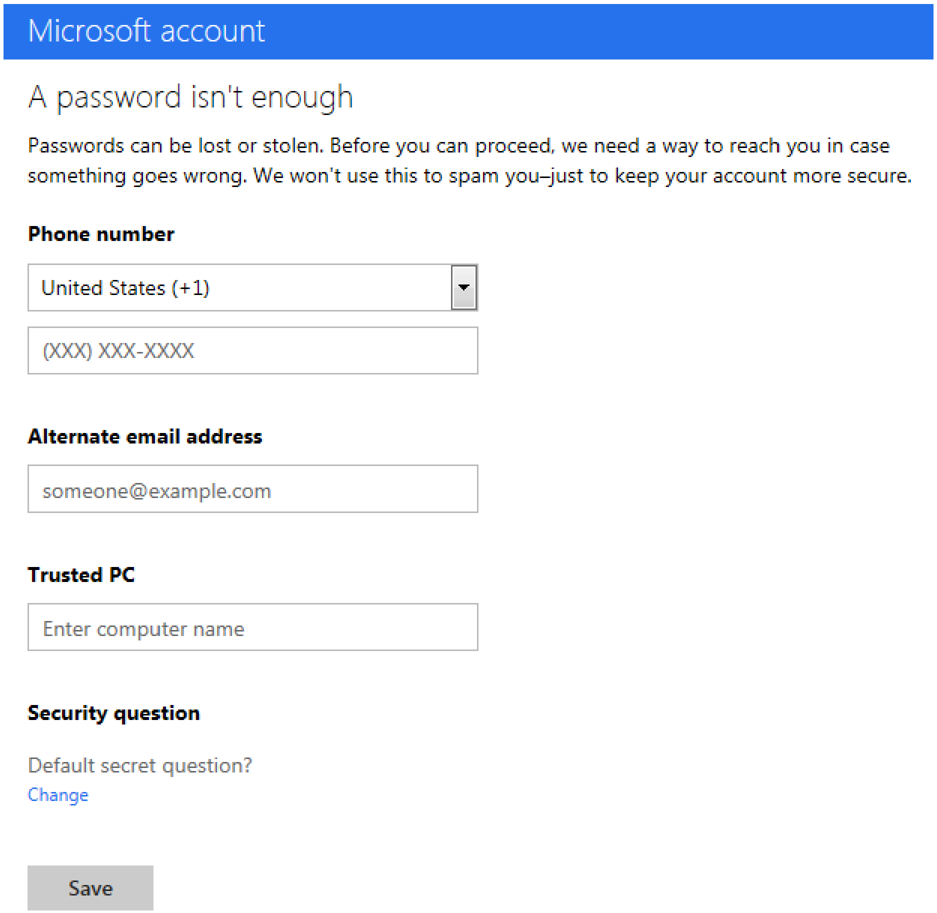
8-character minimum; case sensitive

Reenter password

□ Make me change my password every 72 days

If a user sees a prompt like this, you will want to reset their password to something less common in Active Directory. This is important because passwords from AD will sync to the cloud, but password changes in the cloud will not sync back to AD. If a user were to change their password at this prompt, their password for Live@edu would be different than their password for logging in to the domain. See section 2.14 for additional information on password sync. This will not impact using the SSO at https://mail.kyschools.us.

Users will also see a security prompt from Microsoft to provide additional information to protect their account if they use their Live@EDU credentials to login to any LiveID enabled service other than OWA, such as SkyDrive. Users will be able to supply a security question/answer, phone number, and alternate email address which can be used to recover a compromised account. Users will not be prompted to enter this information by logging into OWA.



Microsoft account

A password isn't enough

Passwords can be lost or stolen. Before you can proceed, we need a way to reach you in case something goes wrong. We won't use this to spam you–just to keep your account more secure.

Phone number

United States (+1)

(XXX) XXX-XXXX

Alternate email address

someone@example.com

Trusted PC

Enter computer name

Security question

Default secret question?
Change

Save

The decision for what type of information should be entered (eg. district phone number or personal phone number) will be up to the district.

Any user who utilizes https://outlook.com, in case of outage of mail.kyschools.us or otherwise, would have to supply their credentials as SSO is not configured (remember that Single Sign-On only functions with https://mail.kyschools.us). However, these credentials are identical to the user's Active Directory credentials, that is to say the user's SMTP Address (UPN) and password (explained above in the section '*User Principal Name login (UPN)'*)

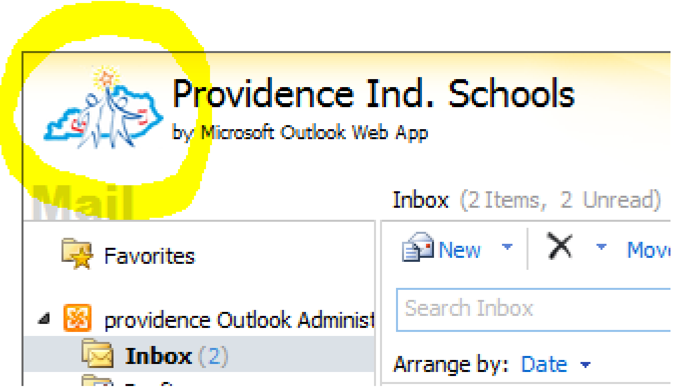
District administrators (or users for that matter) can choose to run Internet Explorer 9 with the –noframemerging switch by editing the shortcut (*"c:\....\iexplore.exe" –noframemerging*). This would allow for multiple versions of IE to be launch with different credential logins to each session. This could be valuable for that that need to login as their normal user credentials and also login as DLAdmin, for instance. Without this switch you would have to close IE and login as the other account. You could also utilize the 'InPrivate' browsing which would open an additional session with no cookies, etc.

For a list of Outlook Web App supported browsers please refer to http://help.outlook.com/en-us/140/bb899685.aspx?ref=search&sl=1

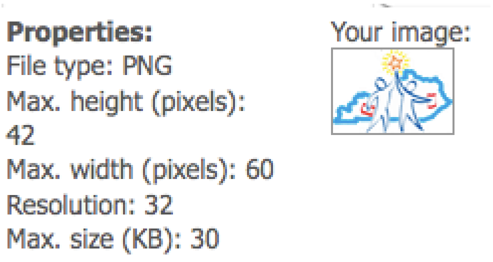
2.10.3 Outlook Live Branding (for OWA)

If the District wishes to 'brand' the Outlook Live Interface (OWA) the follow instructions must be followed. Branding simply refers certain 'customizations' that can be modified in the display users in OWA. There are three different options that can be modified.

Option 1: Modify the image that shows in the top left of the main page.


Providence Ind. Schools
by Microsoft Outlook Web App
Mail
Inbox (2 Items, 2 Unread)
Favorites
New
Movi
Search Inbox
providence Outlook Administ
Inbox (2)
Arrange by: Date

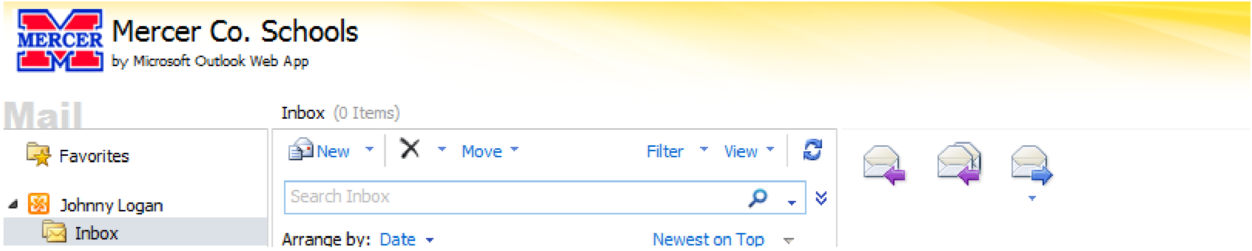
If you wish to change the image displayed on the main OWA page send an email to the KETS Service Desk with an attached PNG image file requesting this change. The image MUST adhere to the following properties (see screen shot below). It is a manual process to change the logo and takes up to 24 hours to publish and update. By default, the KDE logo is
used. If you do not wish to brand OWA for your users the KDE image below will be displayed.



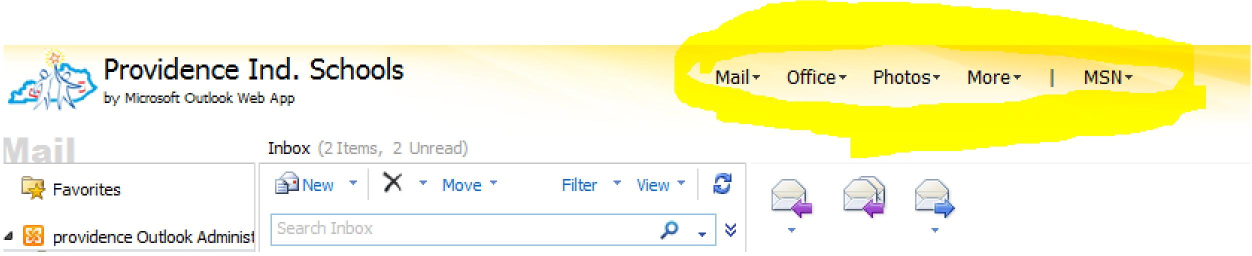
Properties:
File type: PNG
Max. height (pixels): 42
Max. width (pixels): 60
Resolution: 32
Max. size (KB): 30

Option 2: Change the website that users are taken to upon OWA logoff. The default website that users are redirected to when they logout of OWA is http://education.ky.gov. If you want to change this to another website send an e-mail to the KETS Service Desk requesting this change.

Option 3: Modify the 'Menu' bar across the top of the main page in OWA. Districts can choose to either accept the current default of 'no menu bar';



Or elect to have the menu added;


Providence Ind. Schools
by Microsoft Outlook Web App
Mail▾ Office▾ Photos▾ More▾ | MSN▾
Mail
Inbox (2 Items, 2 Unread)
Favorites
providence Outlook Administ
New
Move
Filter
View
Search Inbox

This option can be modified for all Staff and/or Students in a district. Selecting this option will allow users easy access to switch to other collaborative features from within OWA like Skydrive, Office Web Apps, etc.

District should send an e-mail to the KETS Service Desk requesting this change.

2.10.4 MAPI access (Outlook)

Outlook 2007 (and newer), the native client within Snow Leopard (Mac OS X 10.6) and Entourage 2008 WSE (used for Mac OS prior to Snow Leopard) are the only full-featured desktop clients for e-mail access to Outlook Live. Outlook Web App (OWA) is the recommended option for those workstations that do not have the previously stated clients.

Outlook 2007 utilizes a protocol known as 'RPC over HTTP' called Outlook Anywhere for full Outlook (MAPI) access to Outlook Live for e-mail. Since this works over port 443 there are no firewall issues with this client. No previous versions of Outlook are supported for full MAPI functionality. Older versions of Outlook can be configured for IMAP/POP but the experience is less functional than would be experience for Outlook 2007 (or Outlook Web App for that matter).

Since all KETS users have password synced with their Live IDs those that utilize Outlook 2007 will experience 'Same Sign-On'. This means they are required to authenticate with their SMTP address as their login when Outlook loads, but are able to provide their same credentials as they do to login to Active Directory. This assumes that the user will be logging in with their UPN (explained above in section *User Principal Name login (UPN)*).

Outlook 2007 leverages Microsoft's Autodiscover service for new profile creation. When a new user logs into the domain and then launches Outlook for the first time Outlook will take the user's logged in credentials and search DNS for Autodiscover. KIDS has created DNS entries which point these DNS names to Microsoft for resolution. This results in the Outlook client 'finding' the mailbox on the appropriate server at Microsoft to setup the profile.

Note: All mail items in the 'Deleted Items' folder get deleted after 15 days of age.

2.10.5 Mobile Devices

Windows Mobile 6.1 or greater will function with Autodiscover by entering only the SMTP address and password of a user. Some mobile devices will need to be manually configured. Server credentials for mobile devices should be pointed to "**m.outlook.com**". Blackberries may also be configured for IMAP support using "m.outlook.com". Refer to the online documentation at http://help.outlook.com for specific instructions on setting up mobile devices.

2.11 SMTP Relaying

Any district applications which require SMTP relay services should be able to use the relay servers established by KDE. These relay servers accept mail from any authenticated accounts without special intervention. Most applications which use a relay provide a form where you can enter a username and password combination from a service account. With that information, the applications can point to the **ketsmail.us** hostname or **10.16.1.25** IP. If the application/service accepts a URL for the hostname, use "ketsmail.us." For those applications/services that do not accept a hostname/URL use the virtual IP address (VIP) 10.16.1.25.

If a district application/service does not support authentication, first contact the KETS Service Desk requesting IP address access of the application requiring relaying. Once access has been configured, modify those applications to point to **ketsmail.us** for hostname or **10.16.1.25** for static IP. The SMTP services exist at KIDS so in the event that the link to KIDS is down this service will not be functional.

2.12 Exchange Web Services (EWS) and Remote PowerShell

Programmatic/scripted access to Outlook Live and content within Windows Live IDs (mailbox content) are only accessible through Exchange Web Services (EWS) http://msdn.microsoft.com/en-us/library/bb204119.aspx and Remote PowerShell (http://help.outlook.com/en-us/140/cc546278.aspx). The OutlookAdmin account in Student Tenants has access to do many tasks utilizing PowerShell and EWS. There is additionally an OutlookAdmins Security Group which has comparable permissions. OutlookAdmin can add users to this group if desired.

PowerShell and EWS are described in greater detail in Section 3 of this guide. In summary, PowerShell manages objects where EWS manages content within mailboxes (calendar items, mail messages, folders, etc).

There is also an account which specifically exists to run programs under as a 'Service Account' which has permissions to run against the Tenants. These accounts are:

ServiceAdmin@district.kyschools.us (for Staff)

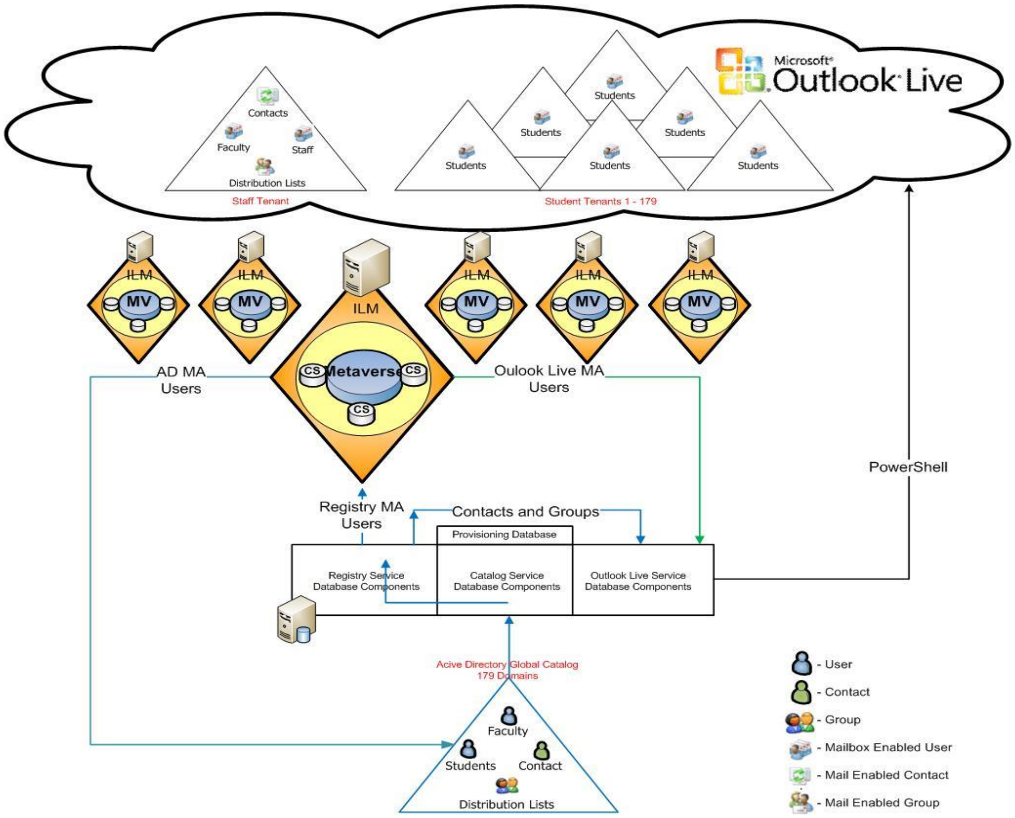
ServiceAdmin@stu.district.kyschools.us (for Students)

where district is the district SMTP Domain Name.

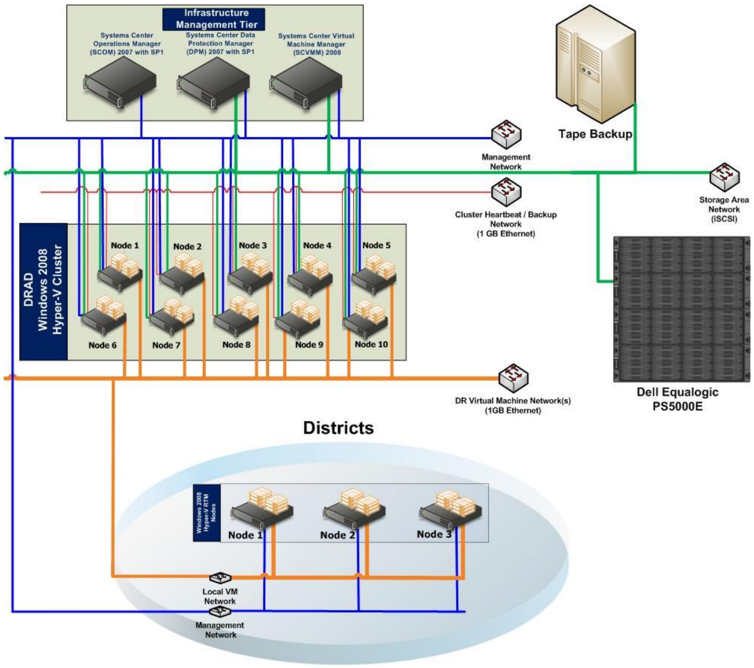
2.13 Online Provisioning System (OLPS) and DR AD

The provisioning system which synchronizes information between KETS Active Directory and Outlook Live is called the Online Provisioning System (OLPS). It is comprised of multiple server instances running Microsoft Identity Lifecycle Manager and other system services. This system is responsible for keeping users, Distribution Groups, Security Groups (if desired) and mail-enabled contacts with certain attributes synchronized with the cloud. Another component of the solution is Password Change Notification Services (PCNS) which keeps passwords in sync between AD and Outlook Live. Any errors which occur will be sent to members of the notifications@*district*.kyschools.us, where district is the district SMTP Domain Name.

There are some administrative tasks which cannot be accomplished with conventional methods so a customized KETS Control Panel exists for those special tasks. These will be explained in greater detail in later sections. The following image is a high-level depiction of the solution.



The OLPS services exist on an environment at KIDS which also contains a backup domain controller for each district domain. This allows OLPS to read from and write to Active Directory at local switch backplane speeds. The system is called DR AD (Disaster Recovery Active Directory). It's a multi-server, SAN solution utilizing Fiber and Windows Server 2008 R2 w/ Hyper-V. District system-state AD backups will be pulled from these servers for disaster recovery. This is a high-level view of the solution:


Infrastructure Management Tier
Systems Center Operations Manager (SCOM) 2007 with SP1
Systems Center Data Protection Manager (DPM) 2007 with SP1
Systems Center Virtual Machine Manager (SCVMM) 2008
Tape Backup
Management Network
Storage Area Network (iSCSI)
Cluster Heartbeat / Backup Network (1 GB Ethernet)
DRAD Windows 2008 Hyper-V Cluster
Node 1
Node 2
Node 3
Node 4
Node 5
Node 6
Node 7
Node 8
Node 9
Node 10
Dell Equalogic PS5000E
DR Virtual Machine Network(s) (1GB Ethernet)
Districts
Windows 2008 Hyper-V RTM Nodes
Node 1
Node 2
Node 3
Local VM Network
Management Network

2.14 Password Synchronization between AD and Outlook Live

Passwords between Active Directory and Outlook Live (through Windows Live ID) are kept in sync through the OLPS system which leverages Password Change Notification Service (PCNS) configured on all KETS Domain Controllers. When a user changes his/her password that password is synced through the OLPS system to the user's Windows Live ID. This allows for the same password to be used between Active Directory and e-mail (whether through Outlook, OWA or mobile devices). If, for any reason, a user changes their password and it doesn't get synced to their Live ID, the user can go to a web portal https://mail.kyschools.us/password.aspx to reset their Outlook Live password to mimic the Active Directory password. Administrators can perform this on behalf of the end users at https://live.kyschools.us/admin.

Note: There can be latency between the time a user changes their Active Directory password and completion of the sync to Outlook Live. During this latency there could be an instance where the user is unable to open Outlook with a newly changed password. (ex. User logs into their machine and changes their password. As soon as the system is up they immediately try to open Outlook). We do not know the scope of this latency at the point of the writing, only enough to say that it could happen and districts should be aware. In this case the user could simply provide their previous password or wait until the synchronization has occurred.

2.15 Availability

2.15.1 Active Directory

In every district there are two Active Directory Domain Controllers housed locally, one being a Global Catalog which is used primarily for Universal Security Group membership lookups at logon. As briefly discussed in the previous section there is an environment at KIDS called 'DR AD' (Disaster Recover Active Directory) which comprises 179 domain controllers, one for each district/sub-domain. This additional domain controller's primary function is for the OLPS system to write changes to Active Directory as well as provide an additional off-site system-state backup for districts of their AD environment.

This off-site AD Domain Controller could be used to service district logins during an outage of the two on-site Domain Controllers if, and only if, district workstations were configured to point to this server as a tertiary (third) DNS entry. This can be accomplished from *Advanced* setting on a NIC. To find the IP address of the Domain Controller that resides in the DR AD environment at KIDS ping:

> **ED***xxx***ADGC2.***districtdomain***.ketsds.net**
>
> Where *xxx* is the district number and *districtdomain* is the district's Active Directory Domain

Note: This off-site domain controller could ***not*** *be used to hand out DHCP addresses. It is only to provide emergency directory server authentication and DNS in a case where both local domain controllers are unresponsive AND the network connection to KDE is available.*

2.15.2 Outlook Live

All user mailboxes and their content are physically located offsite at one of Microsoft's data centers. At the time of this writing there are four data centers across the world. The active mailboxes for KIDS/KDE are all stored in the San Antonio, TX data center which currently allows for the highest capacity. Mailboxes are housed within server 'PODS' that offer triple redundancy. This ensures that if an active mailbox server, or a service, becomes unavailable there are two backups at any given time. Because these data centers hosting this technology exist outside the physical district there are reliance's on other infrastructure components. There are some redundancies built internally like an off-site SSO for OWA, in case the network connection from KIDS/KDE to 'the cloud' is lost. But most components will not be functional if either the network connection for the entire district to the Internet is lost or the connection from the Internet to KIDS/KDE is down.

Below outlines what functionality would be affected if:

> There is a loss of connectivity from a school to the district hub-site or from the district hub-site to the cloud/Internet:
>
> - OWA users would have no access to e-mail
> - Macintosh users would have no access to e-mail
> - Outlook 2007 users would have 'Cache-mode' functionality if configured

- User management within Active Directory would not be synced to Outlook Live while there is an outage. These changes would not be lost and would be provisioned after the connection is established
- Any users who change their AD password while there is an outage may not have their password 'synced' to Outlook Live. If this occurs the end user or administrator would need to access the KETS Control Panel to reset the Outlook Live password

There is a loss of connectivity from KIDS/KDE to the cloud/Internet:

- KETS Control Panel would be down
- https://mail.kyschools.us would not work. Users would need to use https://outlook.com which would require an additional login (but with same AD UPN credentials)
- User management within Active Directory would not be synced to Outlook Live while there is an outage. These changes would not be lost and would be provisioned after the connection is established
- Any users who change their AD password while there is an outage may not have their password 'synced' to Outlook Live. If this occurs the end user or administrator would need to access the KETS Control Panel to reset the Outlook Live password

If there are other outages/connectivity issues outside of the KETS network they could have greater impact, such as affecting handheld devices which rely on other network carriers, etc.

3 Administrative Tasks

3.1 User Administration

The following sections define tasks associated with object management of users, groups and contacts. Some of the tasks can dictate how these objects are provisioned in Outlook Live. Most tasks are handled within Active Directory Users and Computers but a few must be accomplished by other means which are discussed in the next sections. As stated earlier there are four different management avenues for administering Active Directory as it pertains to messaging.

Active Directory administration
Exchange Control Panel
KETS Control Panel
PowerShell / EWS

From a broad level objects are created in Active Directory (users, Security Groups) and provisioned in Outlook Live. The management of those AD objects is done with tools such as Active Directory Users and Computers, DSMOD, etc. The messaging specific tasks such as adding users to Distribution Groups, creating Distribution Groups, changing e-mail properties, etc is done with Exchange Control Panel. KETS Control Panel was created for a few specific tasks which are not easily accomplished through other means. Examples of these tasks are opening another user's mailbox (given you have access), scheduling the provisioning runs between AD and Outlook Live, resetting passwords in case of issues, etc. These are discussed in detail in the following sections, but it is important to note that they are delivered in more of a 'task-based' layout and not grouped in these three areas specifically.

Important Note: *Active Directory / OLPS are authoritative for mail objects that have synced to the cloud. This means that if, for instance, a Distribution Group is created in ADUC and provisioned to Outlook Live a change to that DG (such as name change or membership modification) done in the Exchange Control Panel in OWA would be overwritten by AD the next time that attribute for the DG is synced to Outlook Live. So make sure that objects created in ADUC are managed in ADUC and those created using the Exchange Control Panel should be managed using the Exchange Control Panel. Also note that mailboxes or Distribution Groups created using the Exchange Control Panel in OWA will not be synchronized to AD.*

3.1.1 Active Directory

Active Directory objects (users, groups, etc) can be created using the Active Directory Users and Computers Management Console. This is an excellent method for most management tasks. OU placement can impact how objects are provisioned in Outlook Live for mailbox access. *Example*: If users are created under the Leadership or Staff top-level OUs (or their sub-OUs other than '_Groups') these objects will be provisioned for mailbox access in Outlook Live. They will be placed in the Staff Tenant, meaning they will be a visible member of a single, statewide shared Global Address List. Distribution Group management, on the other hand, can be handled differently than other objects. This is described in following sections.

Very Important Note: *When a new user object is created, by any technical means, that object must initially be provisioned through the OLPS system and THEN the password must be changed/reset in AD to allow the password to be synced to Outlook Live. Districts should delay giving the user their credentials up to 2 hours as it could take that long for OLPS to write the SMTP address to the AD UPN for the user, thus allowing them to know their SMTP address and possibly what to login as. When the 'E-mail' attribute is populated on the General tab for a user in ADUC the object has been provisioned and it is safe to give the user their login credentials and have them change their password*

District administrators can do one of two procedures as it pertains to the initial password sync:

1. *Create account, set a temporary password and set to force the user to change the password on next login. This can be done through ADUC or by setting the Active Directory pwdLastSet attribute to 0 (zero) on the user(s). There must be at least a 2 hour delay between creation and password set to allow the object to be provisioned. This 'delay' is also needed to allow OLPS to write the SMTP Address back to the UPN value of the user. This allows the user to login to the workstation/domain with their SMTP Address.*
2. *Create accounts with the desired password, and then from KETS Control Panel set the password in Outlook Live to match the Active Directory password. This can be done by an admin. If the user ever changes their AD password in the future PCNS will pass the change to Outlook Live.*

Other means exist for administering objects in AD, such as CSVDE, LDIFDE, DSADD/DSMOD, PowerShell as well as other scripting mechanisms and third-party applications. District administrators should reference resources on the internet as well as other publications to assist with these technologies. Administrators should understand and possibly utilize the KETS Active Directory attributes discussed in section *KETS Specific Attributes and Active Directory Attribute Flow.*

Online Provisioning System (OLPS) will provision these newly create objects in AD into Outlook Live. It is configured to run every 15 minutes for Staff mailboxes. This means that, by default, it can take up to 1 hour (with replication latency, etc) before a Staff user's mailbox is created in Outlook Live (*6 hours for Students*). This also applies to any modification of users between AD and Outlook Live (attribute changes, etc).

Note: User deletions are only provisioned once each night. Group creations and modifications (membership in AD, etc) would also take overnight before the change is made in Outlook Live. Group and Contact deletions are once per week.

A member of DIST Support Admins can disable the scheduled run of provisioning through the KETS Control Panel (https://live.kyschools.us/admin). This might be useful if districts are going to perform a bulk amount of changes in Active Directory (like create student accounts at the beginning of the school year). Districts may want to turn off the scheduled run, make all of the creations/modifications, and when all changes are complete turn on provisioning.

Mass user creations/modifications should be performed at the end of the day, preferably not on Mondays. This is stated because Mondays will be popular across the state for password changes as folks an entire district could be forced to all change their passwords in the mornings. These tasks being performed by the OLPS system would compete with a district trying to create possibly 1,000 or more user objects. Creating or modifying many objects at once is best to do off-hours, or at least toward the end of a day.

It's important to note that the DIST Staff or Student Deleted Mailbox and DIST Staff or Student Locked Mailbox groups within Active Directory Users and Computers are NOT used for disabling mailbox provisioning. These groups are legacy Exchange 2003 groups and have been left in case the district chose to utilize these Security Groups for other purposes. The proper steps to set or restrict mail access are outlined below.

There are three ways that a user/group/contact object can be created or assigned so that OLPS will provision it properly in Outlook Live.

1 – Place AD objects in the proper Organization Unit.

- Any user created in the Leadership or Staff top-level OUs (or sub-OUs other than _*Groups*) will be assigned a *KETS User Type* of 'Staff' and placed in the Staff Tenant (GAL) in Outlook Live.
- Users placed in the Student top-level OU (or sub-OUs other than _*Groups*) will be assigned a *KETS User Type* of 'Student' and placed in the Student Tenant (GAL).

  IMPORTANT NOTE: *If a user is created in AD in one top-level OU (ex. Student) and then moved to another top-level OU (ex. Staff) OLPS will not recognize this occurrence. The KETS User Type on the 'KETS EDU' tab would need to be manually modified to the proper designation (Staff, Student or Resource). This would result in a new Live ID and mailbox for that user as they would be 'moving' to a different 'Tenant'.*

2 – Assign values to the attributes on the *KETS EDU* tab in ADUC*. The first two attributes (*District Code* and *System ID*) are reserved by the system.

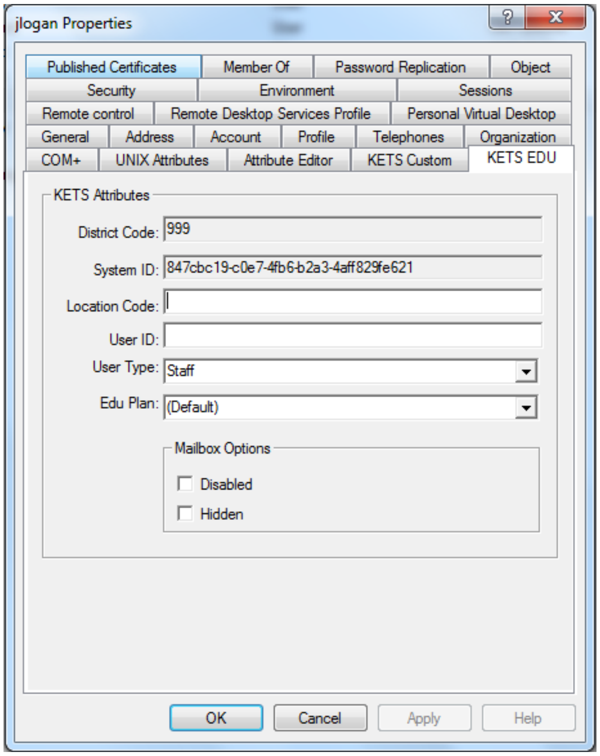
- **Location Code** – Value that can be up to 255 characters at the discretion of the district. This attribute is not used by the system. It exists for the district to standardize if they so choose.
- **User ID** – Reserved by the system. Will possibly be used in the future. We have enabled it in ADUC so it will be available if implemented. Leave blank for now.
- **Edu Plan** –
  - Leaving this field as *(default)* will result in a mailbox being created in Outlook Live. This is the default setting and does not need to be stamped on every user account.
  - A choice of ***NoMail*** will result in an account that is not synchronized with Outlook Live, but it will provision the SMTP to be written back to AD, allowing for login with the SMTP Address (UPN).

    Important Note: *If a mailbox has been previously provisioned for the user, changing the selection to NoMail will result in the mailbox in Outlook Live being* ***purged*** *upon the next run of OLPS provisioning. The* *operation bypasses the Tombstones! Please use this setting with caution. A choice of NoMail will result in one of two things:*

    - If no mailbox currently exists for the user OLPS will not create a mailbox.
    - If a mailbox currently exists for the user OLPS would purge the mailbox, bypassing the tombstones.

- **Edu Disabled** - A choice of Disabled (checked) will result in the mailbox in Outlook Live being disabled upon the next run of OLPS provisioning (up to 1 hour). This option prevents end-user access to their mailbox, but preserves mail-flow into the mailbox and does NOT disable the AD object. ***Also, if the user object itself is disabled in ADUC the mailbox will also be disabled.***
- **Edu Hidden** - A choice of Hidden (checked) would result in the mailbox in Outlook Live being hidden from the GAL. For Students this will be set automatically in OLPS. You should disregard this attribute for Students.
- **User Type** – The user type is automatically calculated by OLPS based on the user account positioning in the containers. You will not need to stamp this attribute unless you plan to override the default. For example, a user account in either the Leadership or Staff containers will be assigned a value of Staff for this attribute. Similarly, a user account in the Students container will be assigned a value of Student for this attribute. Thus, the intention of this attribute is to view the assigned value as opposed to altering it. In some cases you may choose to if user accounts are placed in different containers, but do so with caution.
    - A choice of *Staff* would result in the mailbox being created in the Staff Tenant (GAL) if **Edu Plan** is 'blank'.
    - A choice of *Student* would result in the mailbox being created in the Student Tenant (GAL) if **Edu Plan** is 'blank'
    - A choice of *Resource* would prompt OLPS to take no action

        Note: This can be useful for accounts like 'Lab1' etc where computers in a student lab are logged into AD as a resource account, but students need to access OWA. If the 'Lab1' AD user object has a mailbox, OWA through SSO will log the mailbox 'Lab1' into mail instead of prompting for the student credentials. In this example, the district would want to either place the 'Lab1' type accounts into the _Groups OU or chose 'Resource' for User Type.



KETS Attributes

District Code: 999

System ID: 847cbc19-c0e7-4fb6-b2a3-4aff829fe621

Location Code:

User ID:

User Type: Staff

Edu Plan: (Default)

Mailbox Options

☐ Disabled

☐ Hidden

3 – Assign values to the attributes of objects through programmatic means (LDIFDE, PowerShell, etc) against Active Directory. The attribute names and descriptions are outlined in the section entitled '*KETS Specific Attributes and Active Directory Attribute Flows*'.

Special Note: *If a value of 'NoMail' is set for EDU Plan for a given user (or users) and the desire is enable a mailbox you would select '(Default)' in ADUC. If you are using script to modify numbers of users (ex. Students are set to 'NoMail' at beginning of summer to delete their mailbox, then before schools starts the desire is to recreate new mailboxes) you can set the attribute 'ketsEDUPlan' to 'MailOnly', or simply delete the value which will set to (Default).*

Mail objects can also be created in Outlook Live directly through the Exchange Control Panel or Remote PowerShell, but these will bypass the special provisioning/tagging that is built into OLPS, as the accounts would not exist in Active Directory. As long as there is no need to have a corresponding Active Directory user account for the desired mailbox (Conference Room, for instance) creating the mailbox with Exchange Control Panel is fine.

* The installer for ADUC to show these additional tabs can be found at http://education.ky.gov/districts/tech/tss/Pages/default.aspx > then select (KETS Email Services) and (Install Files).

Note: The 32-bit version (KETSEdu_ADUC_32bit.msi) is for any 32-bit OS. The 64-bit version (KETSEdu_ADUC_64bit.msi) works for Windows Server 2008 64-bit and Windows 7 64-bit. 64-bit operating systems other than those specified will not show the 'Attribute Editor' tab. The 'Attribute

Editor' tab (available with the Microsoft Remote Server Administration Tools (RSAT)) is to be used to read/modify the extensionAttibutes (aka Custom Attributes). These are attributes that were part of the legacy Exchange 2003 system which some districts chose to utilize. PLEASE be cautious while in Attribute Editor as IT Admins have the permission to modify many of the Active Directory attributes while in this tab, which could cause ill effect. It's also important to note that districts have 15 additional attributes (ketsCustom1 – ketsCustom15) that can be used as the district sees fit. These are explained later in the sections entitled 'KETS Specific Attributes and Active Directory Attribute Flows'.

Important Note: *If you have installed the above stated apps and still do not see the Attribute Editor tab you should create a shortcut on your desktop with the following:*

```
%SystemRoot%\System32\mmc.exe -32 %SystemRoot%\system32\dsa.msc
```

The -32 switch should display the Attribute Editor tab

3.1.2 Deletion of Active Directory User Objects

When deleting Active Directory user object that have a corresponding Windows Live ID and mailbox, one should think about the desired outcome of access to mail for the given user. If a user object is deleted in ADUC, the corresponding mailbox would still receive mail until the tombstone days have expired, at which time the mailbox and Windows Live ID will be deleted. This is the case for Staff and Students. Staff, by default, do not have access to their mailbox after the AD object is deleted, *but the mailbox will still show in the Global Address List and receive mail*. Students have access to open their mailboxes, again by default, after AD user object deletions until the tombstone days expire (90 days by default). Districts can modify these settings on the 'District Config' section of the KETS Control Panel logged in as a member of DIST Support Admins.

Districts may choose to set the user object to 'Hidden' on either the AD object on the KETS EDU tab before deletion, or through PowerShell. An example of this is shown later in this document under 'PowerShell – Examples – Hide Mailbox'.

A district could also choose to set 'NoMail' on the KETS EDU tab of the user, wait for that to provision through the system, and then delete the AD user object. Note that setting 'NoMail' will immediately delete the mailbox.

3.1.3 Re-Creation of Active Directory User Objects

It is important to know that if a district chooses to recreate user objects (ex. Delete all student AD objects at end of school year and recreate all before school starts) the old/original e-mail address would need to be populated upon recreation for the AD objects to 'join' to the Windows Live IDs. If this is not done the provisioning system will create new Windows Live IDs for all students, appending a numerator at the end of the prefix.

As an example of we have a student AD object *12bobby* whose SMTP is 12bobby@providence.kyschools.us . If we delete his AD user object we have, by default, 90 days of tombstone time before the Windows Live ID and corresponding mailbox is purged. During this time we can create a new AD object for *12bobby,* but to join this new AD object with the Windows Live

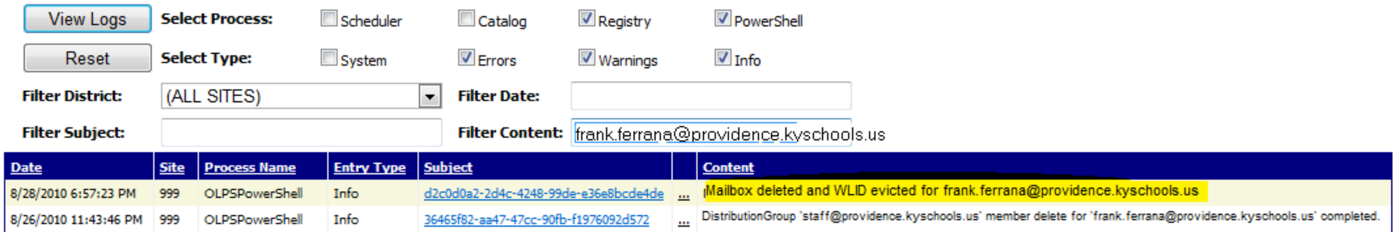
ID/mailbox that's tombstoned we would have to specify the e-mail address 12bobby@providence.kyschools.us to force the provisioning system (OLPS) to join this AD object to the tombstoned mailbox. If the E-mail attribute is not specified OLPS will simply look for the next available SMTP address, create a new Windows Live ID and mailbox (ex. 12bobby2@providence.kyschools.us).

3.1.4 Preventing Incremented SMTP Addresses for New Users

If a new user object is created in Active Directory, when a previous user object existed with the same first and last name, OLPS will stamp an incremented SMTP address on the new object.

For example, a staff member named Frank Ferrana leaves the district and his AD user object is deleted. His SMTP address frank.ferrana@providence.kyschools.us is stored in OLPS forever. Later, a new staff member with the same name is hired, and has an AD user object created. He will be stamped with an SMTP address of frank.ferrana2@providence.kyschools.us. This can be prevented by using the following method.

Method: New user starts today named Frank Ferrana. Go to KETS Control Panel and search for frank.ferrana@providence.kyschools.us.



Select Process: □ Scheduler □ Catalog ☑ Registry ☑ PowerShell

Select Type: □ System ☑ Errors ☑ Warnings ☑ Info

Filter District: (ALL SITES)

Filter Date:

Filter Subject:

Filter Content: frank.ferrana@providence.kyschools.us

Date	Site	Process Name	Entry Type	Subject		Content
8/28/2010 6:57:23 PM	999	OLPSPowerShell	Info	d2c0d0a2-2d4c-4248-99de-e36e8bcde4de	...	Mailbox deleted and WLID evicted for frank.ferrana@providence.kyschools.us
8/26/2010 11:43:46 PM	999	OLPSPowerShell	Info	36465f82-aa47-47cc-90fb-f1976092d572	...	DistributionGroup 'staff@providence.kyschools.us' member delete for 'frank.ferrana@providence.kyschools.us' completed.

If you see that he had existed, and mailbox and Live ID have been evicted (deleted in the screenshot above) you could create the new user in AD and then immediately set the 'Email Address' on the General tab in ADUC with frank.ferrana@providence.kyschools.us. The provisioning system will create a new Live ID and SMTP address that is not incremented. If the search for frank.ferrana@providence.kyschools.us shows no entries in the Logs the district could simply create the user in AD, and allow OLPS to provision the user object.

If having an incremented SMTP address is not a concern, the Active Directory user object can be created as usual, with no extra steps required.

3.1.5 Distribution Group Administration

Distribution Group administration in Outlook Live is handled differently than management of user objects. It is suggested to do all Distribution Group administration through the Exchange Control Panel (accessible from www.outlook.com > Options). You must be logged in as either DLAdmin@*district*.kyschools.us or DLAdmin@stu.*district*.kyschools.us, where *district* is your district's SMTP suffix name. Districts do have the ability to create groups in Active Directory, which would provision through OLPS to Outlook Live. However there are certain tasks that can only be performed for DGs in Exchange Control Panel (such as setting ownership, permissions, etc).

Note: Groups created in Active Directory must be set as 'Universal' Groups if they are to be provisioned to Outlook Live. This is because the group membership for Universal Groups is replicated throughout AD so that OLPS can pick them up to provision.

The different scenarios of Distribution Group management are outlined in the following sections. Also, if the desire is to allow staff in a district to manage Distribution Groups (such as adding membership) this group must be created in the Exchange Control Panel.

Note: If a DG is created in AD and membership is modified in Outlook Live the membership will be overwritten by AD the next time the group is modified in AD. This is why it is suggested to use Exchange Control Panel to create and manage groups whenever possible.

If a district chooses to have an Active Directory Security Group that also has a corresponding Distribution Group you should create the Security Groups in Active Directory Users and Computers (ADUC) as a 'Universal' Group and then enter an e-mail address for the group in the 'E-mail' field on the General tab. This will trigger OLPS to create a Distribution Group in Outlook Live for the group. Groups in Active Directory which require an Outlook Live Distribution Group must NOT exist in any _Groups OUs. OLPS does not look at objects in these OUs. Ownership or permissioning of who can send to the group, however, will not be synchronized to Outlook Live. Those settings must be set in Exchange Control Panel. Distribution Groups in AD must also have the E-mail address populated in AD. It is suggested to create Distribution Group in Exchange Control Panel instead of ADUC.

DLAdmin@district.kyschools.us and DLAdmin@stu.district.kyschools.us are automatically set as 'Owner' of any Distribution Group that's created in Outlook Live. The DLAdmin will need to add additional users as 'Owner' if that's desired. Owner's can perform tasks such as Enable Message Approval, Change Group Properties in Exchange Control Panel, use Remote PowerShell to manage groups, set who can send to the group, etc. Steps required to perform these tasks as well as others can be found by searching http://help.outlook.com.

Note: Distribution Groups or Contacts do NOT flow to the Student Outlook Live Tenant from AD. Distribution Groups and Contacts have to be created with ECP or PowerShell in the Student Tenant. Remember that Students currently do not see objects in their Global Address List.

There are certain 'Statewide Shared' Distribution Groups that districts should continue to maintain membership of, such as 'Allen Co Teachers' or 'Pineville Ind Principals'. These Distribution Groups are nested under top-level DGs such as 'All State Teachers', which are used for mass mailings by selected individuals (Commissioner of KDE, etc). Districts can look at the 'Member of' tab on these suspected DGs to see the nesting if there are question.

Important Note: *A single Outlook Live mailbox can only send to 3,000 individual recipients per day. However, Distribution Groups only count as one recipient. If a district has users, say a superintendent or principal, that need to send 'bulk' e-mails they should utilize Distribution Groups. Make sure that these DGs are limited as to who has permissions to send to them. ALSO, any time a user sends to large numbers of recipients they should adopt adding that Distribution Group/recipients to the 'BBC' field in the new mail form instead of the' To' field. The sender should add themselves to the 'To' field. This is reiterated again later in this document, but it warrants repeating as using this mechanism restricts recipients from clicking 'Reply All' as the BBC field is not used on a 'Reply All'.*

3.1.5.1 Staff - Distribution Group Administration

For Staff it is recommended to create Distribution Groups in Exchange Control Panel (https://outlook.com/ecp or OWA > Options). As stated previously districts could create groups in

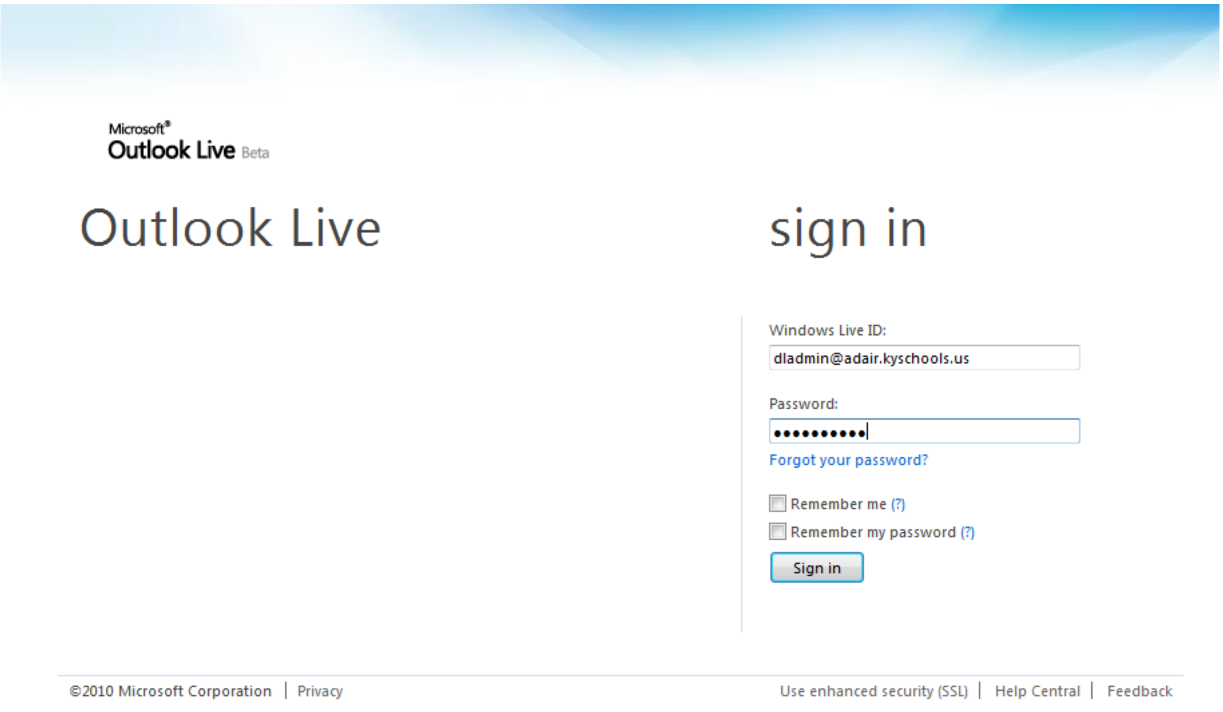
Active Directory if desired but certain aspects of management would have to be performed in the Exchange Control Panel. The IT Admin would need to login as DLAdmin@*district*.kyschools.us, where *district* is the district's SMTP domain suffix name.

www.outlook.com should be utilized for any 'administrative' tasks that need to be performed in the Exchange Control Panel instead of using mail.kyschools.us. The reason for this is mail.kyschools.us will use the Active Directory credentials of the user logged in to the workstation. For using accounts such as DLAdmin@..., OutlookAdmin@... Etc, you will need to login to www.outlook.com as the Windows Live ID of those users, as they do not exist in Active Directory.

Note: A Security Group requiring an equivalent Distribution Group which is created in Active Directory Users and Computers, OR a Distribution Group created in AD, will need to have the 'E-mail' field on the General tab populated with the desired SMTP address for OLPS to provision the group as a Distribution Group in Outlook Live. These groups can NOT exist in any OU named '_Groups' as these are ignored by OLPS. This e-mail address must be accurate as far as the suffix (ex. …@adair.kyschools.us) to be created properly.

Distribution Groups are visible to all staff in the state and are, by default, open for any staff in the state to send to. The corresponding DLAdmin account is set as 'Owner' of each district's Distribution Group. Certain tasks like modifying ownership, restricting who can send to the Distribution Group, etc. are performed through the Exchange Control Panel (either through Outlook Web App logged in as the DLAdmin account or through https://outlook.com/ecp).

Login to outlook.com, click on 'Options' to the top right

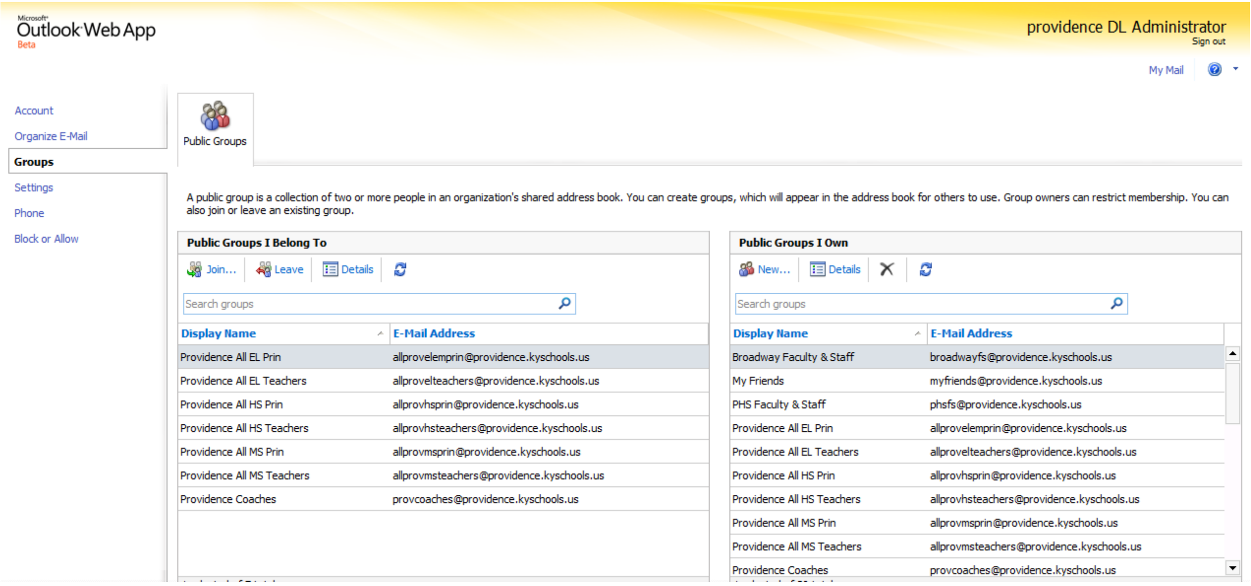


Microsoft® Outlook Live Beta
Outlook Live
sign in

Windows Live ID: dladmin@adair.kyschools.us

Password: ●●●●●●●●●●

Forgot your password?
□ Remember me (?)
□ Remember my password (?)
Sign in
©2010 Microsoft Corporation | Privacy
Use enhanced security (SSL) | Help Central | Feedback



Microsoft Outlook Web App Beta

providence DL Administrator
Sign out

My Mail

A public group is a collection of two or more people in an organization's shared address book. You can create groups, which will appear in the address book for others to use. Group owners can restrict membership. You can also join or leave an existing group.

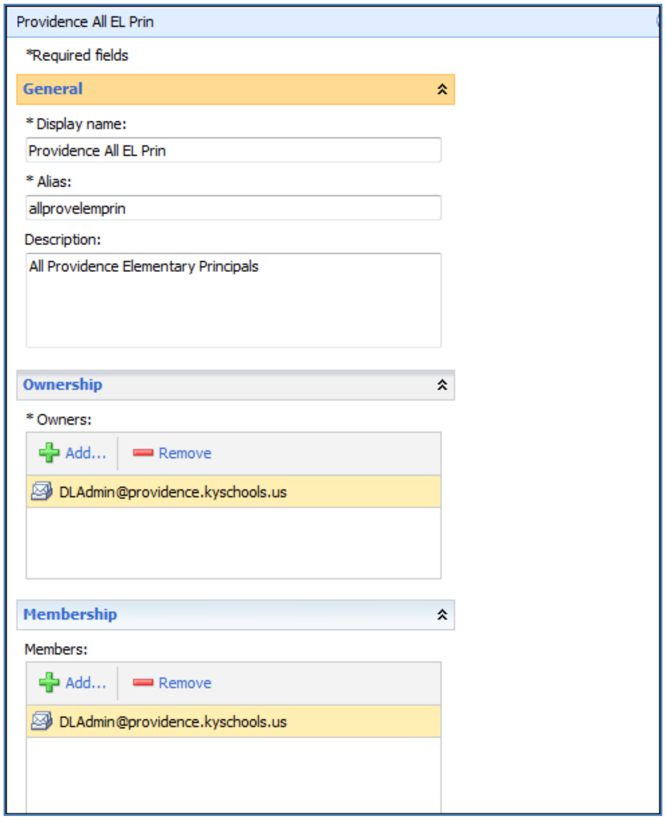
Public Groups I Belong To

Display Name	E-Mail Address
Providence All EL Prin	allprovelemprin@providence.kyschools.us
Providence All EL Teachers	allprovelteachers@providence.kyschools.us
Providence All HS Prin	allprovhsprin@providence.kyschools.us
Providence All HS Teachers	allprovhsteachers@providence.kyschools.us
Providence All MS Prin	allprovmsprin@providence.kyschools.us
Providence All MS Teachers	allprovmsteachers@providence.kyschools.us
Providence Coaches	provcoaches@providence.kyschools.us

Public Groups I Own

Display Name	E-Mail Address
Broadway Faculty & Staff	broadwayfs@providence.kyschools.us
My Friends	myfriends@providence.kyschools.us
PHS Faculty & Staff	phsfs@providence.kyschools.us
Providence All EL Prin	allprovelemprin@providence.kyschools.us
Providence All EL Teachers	allprovelteachers@providence.kyschools.us
Providence All HS Prin	allprovhsprin@providence.kyschools.us
Providence All HS Teachers	allprovhsteachers@providence.kyschools.us
Providence All MS Prin	allprovmsprin@providence.kyschools.us
Providence All MS Teachers	allprovmsteachers@providence.kyschools.us
Providence Coaches	provcoaches@providence.kyschools.us

You will notice that the window on the right says "Public Groups I Own". As DLAdmin for each district is set to Owner of all district DGs you will have the ability to manage them here.



Providence All EL Prin

*Required fields

General

* Display name: Providence All EL Prin

* Alias: allprovelemprin

Description: All Providence Elementary Principals

Ownership

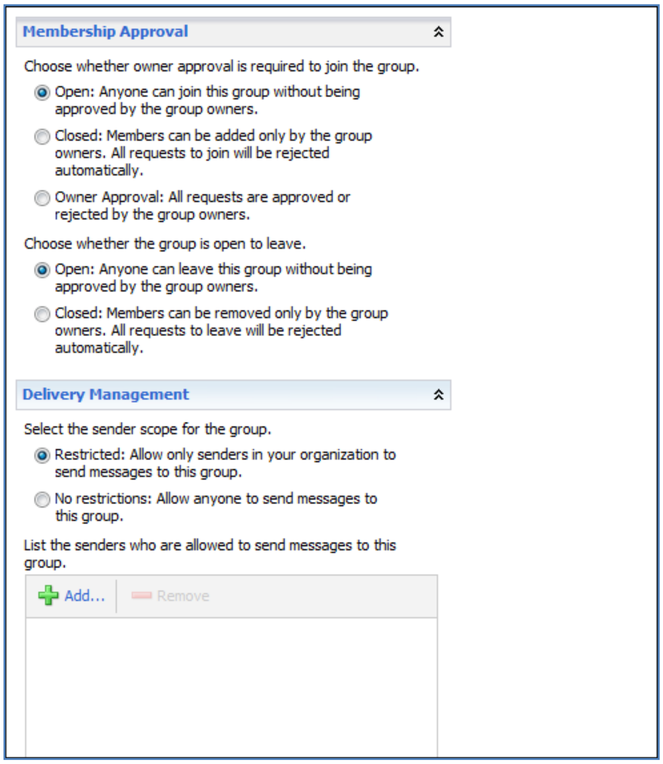
* Owners:

DLAdmin@providence.kyschools.us

Membership

Members:

DLAdmin@providence.kyschools.us



Membership Approval

Choose whether owner approval is required to join the group.

● Open: Anyone can join this group without being approved by the group owners.

○ Closed: Members can be added only by the group owners. All requests to join will be rejected automatically.

○ Owner Approval: All requests are approved or rejected by the group owners.

Choose whether the group is open to leave.

● Open: Anyone can leave this group without being approved by the group owners.

○ Closed: Members can be removed only by the group owners. All requests to leave will be rejected automatically.

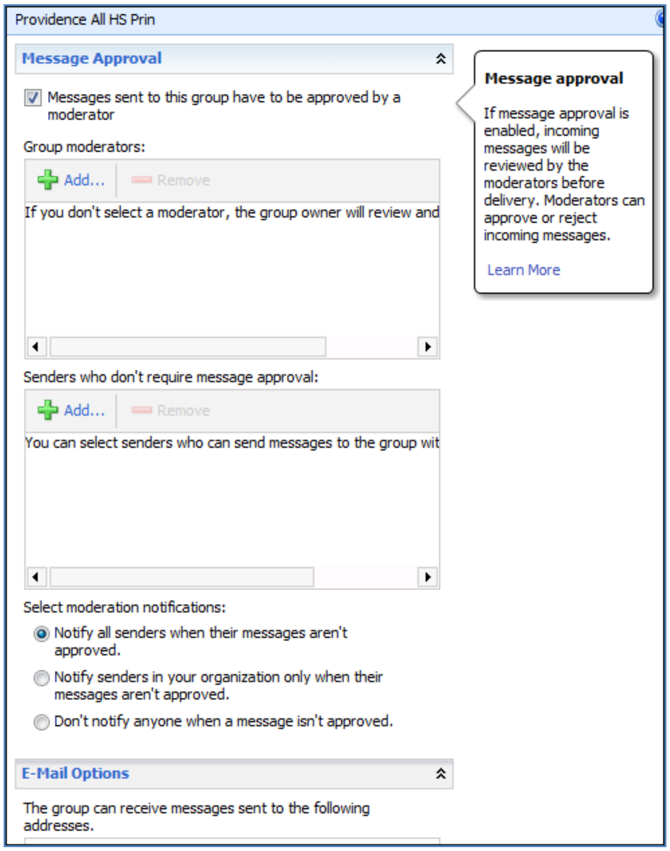
Delivery Management

Select the sender scope for the group.

● Restricted: Allow only senders in your organization to send messages to this group.

○ No restrictions: Allow anyone to send messages to this group.

List the senders who are allowed to send messages to this group.



Providence All HS Prin

Message Approval

☑ Messages sent to this group have to be approved by a moderator

Group moderators:

If you don't select a moderator, the group owner will review and

Senders who don't require message approval:

You can select senders who can send messages to the group wit

Select moderation notifications:

● Notify all senders when their messages aren't approved.

○ Notify senders in your organization only when their messages aren't approved.

○ Don't notify anyone when a message isn't approved.

Message approval

If message approval is enabled, incoming messages will be reviewed by the moderators before delivery. Moderators can approve or reject incoming messages.

Learn More

E-Mail Options

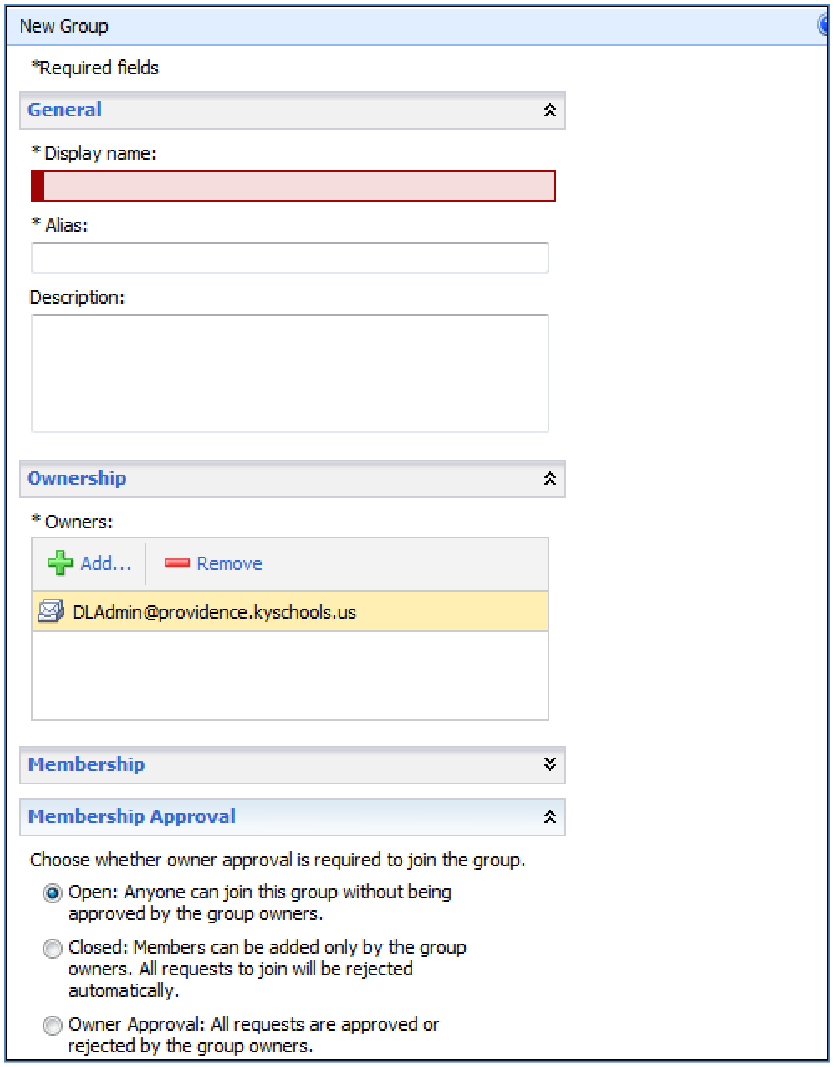
The group can receive messages sent to the following addresses.

A couple of interesting features to point out are Message Approval and the ability for users to add themselves as members to DGs. Notice above that if the DG is set for 'Message Approval' you can specify the moderator, who would have all messages sent to the DG first sent to them for approval or rejection. You can also select users who would not have their messages 'moderated'.

Another extremely valuable feature which exists in Outlook Live for Distribution Group which was not available in previous versions of the KETS Exchange System is the ability to create DGs which are *'Opened'* or *'Owner Approved'*. This means that a group can be set any of three ways for membership.

1. **Closed**: Member can only be added by an Owner of the group
2. **Open:** Any user can add themselves to the group
3. **Owner Approval**: Requests to be added are sent to group Owners. First Owner to approve or deny wins.

Important Note: Groups that are created in Active Directory (DGs or SGs) are created in Outlook Live as 'Closed'. Those created using Exchange Control Panel are set to 'Open' as default, meaning any users can add themselves to the group.


New Group

*Required fields

General

* Display name:

* Alias:

Description:

Ownership

* Owners:

Add... | Remove

DLAdmin@providence.kyschools.us

Membership

Membership Approval

Choose whether owner approval is required to join the group.

● Open: Anyone can join this group without being approved by the group owners.

○ Closed: Members can be added only by the group owners. All requests to join will be rejected automatically.

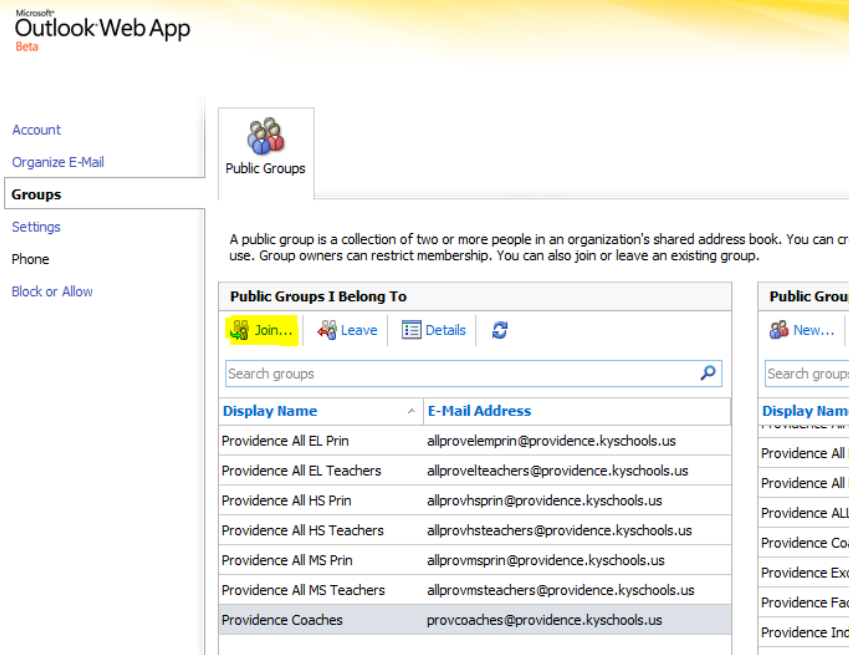
○ Owner Approval: All requests are approved or rejected by the group owners.

Note: If the DLAdmin account password needs to be reset, contact the KETS Service Desk.

3.1.5.1.1 How Users Join Groups that are 'Open' or 'Owner Approval'

The purpose of this guide is not to define end-user processes to perform every task, but as this particular discussion is a 'new' technology, a screen shot was thought helpful. *There is no support from an Outlook client for a user to add (or request add) themselves to a group, this can only be done using OWA.*

From OWA, a user would select 'Options' from the top right of the screen which would result in the screen below which is in the background. They would then select 'Groups' as shown below. Notice just to the left of the 'active' window it shows *Public Groups I Belong To* which has a *Join…* button below it. The *Join…* button is what they would want to click on to open the active window you see below, but the confusing part it that the button has nothing to do with the *Public Groups I Belong To* area in which it resides. Obviously a user wouldn't need to join a group they already belong to, which is what this window appears to show. Users would, however, user the *Leave* button (shown as inactive below) if they wanted to leave the membership of a DL. They would select the DG they want and click *Leave*.



A public group is a collection of two or more people in an organization's shared address book. You can cr
use. Group owners can restrict membership. You can also join or leave an existing group.

Public Groups I Belong To

Display Name	E-Mail Address
Providence All EL Prin	allprovelemprin@providence.kyschools.us
Providence All EL Teachers	allprovelteachers@providence.kyschools.us
Providence All HS Prin	allprovhsprin@providence.kyschools.us
Providence All HS Teachers	allprovhsteachers@providence.kyschools.us
Providence All MS Prin	allprovmsprin@providence.kyschools.us
Providence All MS Teachers	allprovmsteachers@providence.kyschools.us
Providence Coaches	provcoaches@providence.kyschools.us

Public Grou

Display Nam
Providence All
Providence All
Providence ALL
Providence Co
Providence Ex
Providence Fa
Providence Inc

3.1.5.2 KETS State-wide Shared Distribution Group Permissioning

The following Distribution Groups are sponsored by KDE and School Districts and are to be provisioned properly to allow for certain individuals (KDE Commissioner, etc) to send to the members. **Membership is to be properly maintained by the district.** District have the flexibility to add additional permission if they so choose.

To assign access rights to each distribution list, go to the Options link inside OWA (with the DLAdmin account), go to "Groups" and "Public Groups I Own" and follow the steps outlined below.

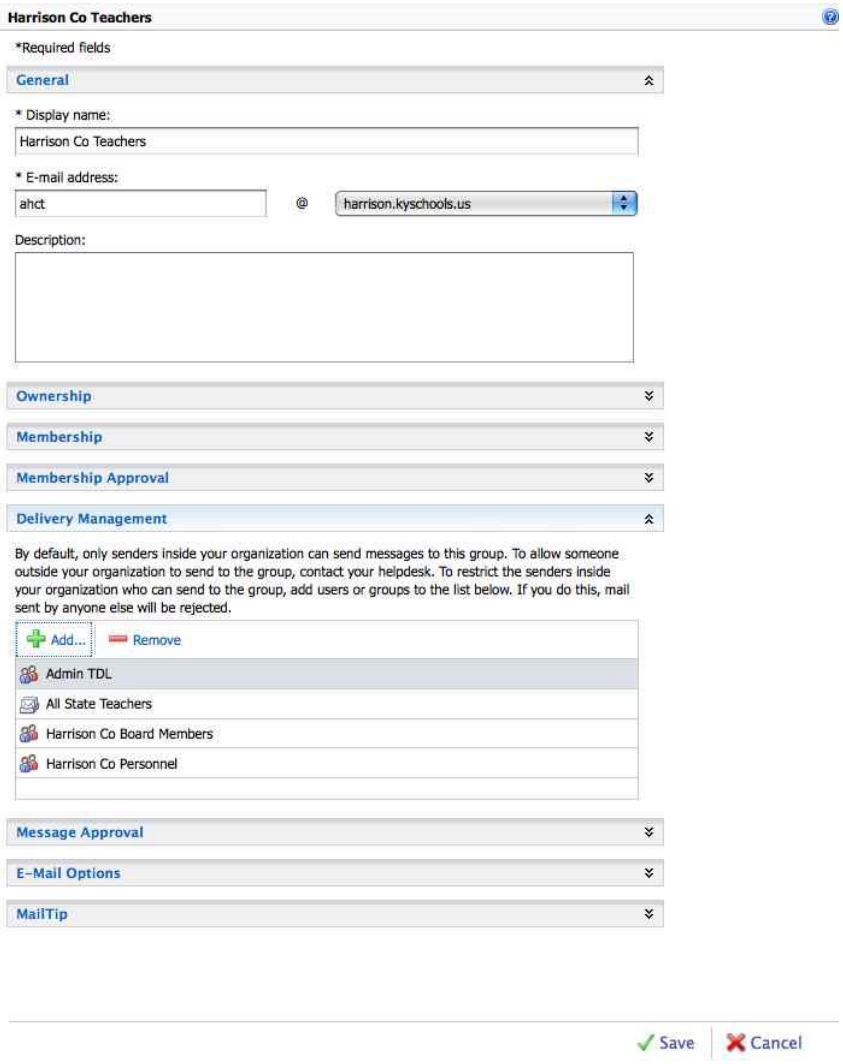
Note: If no one is listed in Delivery Management, everyone can send to the group; if there is a user or group listed in the Delivery Management only the members (not nested members) can send in to the group. (see screen shot below)

- **For All *District Name* Supt:** Click on "Delivery Management" and add *"All State Supt" and "Admin SDL" as well any additional user or group in your district that should send; Click Save.*
- **For All *District Name* Prin:** Click on "Delivery Management" and add *"All State Prin" and "Admin PDL" as well any additional user or group in your district that should send. Example: "**All Adair Principals**" or **"Doe, Joe";** Click Save.*
- **For All *District Name* EL Prin:** Click on "Delivery Management" and add *"All State Prin" and "Admin EPDL" as well any additional user or group in your district that should send. Example: "**All Adair El Principals**" or **"Doe, Joe";** Click Save.*
- **For All *District Name* MS Prin:** Click on "Delivery Management" and add *"All State Prin" and*

*"Admin MPDL" as well any additional user or group in your district that should send. Example: "**All Adair MS Principals**" or **"Doe, Joe";** Click Save.*

- **For All *District Name* HS Prin:** Click on "Delivery Management" and add *"All State Prin" and "Admin HPDL" as well any additional user or group in your district that should send. Example: "**All Adair HS Principals**" or **"Doe, Joe";** Click Save.*
- **For All *District Name* Teachers:** Click on "Delivery Management" and add *"All State Teachers" and "Admin TDL" as well any additional user or group in your district that should send. Example: "**All Adair Teachers**" or **"Doe, Joe";** Click Save.*
- **For All *District Name* EL Teachers:** Click on "Delivery Management" and add *"All State Teachers" and "Admin ETDL" as well any additional user or group in your district that should send. Example: "**All Adair EL Teachers**" or **"Doe, Joe";** Click Save.*
- **For All *District Name* MS Teachers:** Click on "Delivery Management" and add *"All State Teachers" and "Admin MTDL" as well any additional user or group in your district that should send. Example: "**All Adair MS Teachers**" or **"Doe, Joe";** Click Save.*
- **For All *District Name* HS Teachers:** Click on "Delivery Management" and add *"All State Teachers" and "Admin HTDL" as well any additional user or group in your district that should send. Example: "**All Adair HS Teachers**" or **"Doe, Joe";** Click Save.*
- **For All *District Name* IT Teachers (for District Itinerant teachers):** Click on "Delivery Management" and add *"All State Teachers" and "Admin ITDL" as well any additional user or group in your district that should send. Example: "**All Adair IT Teachers**" or **"Doe, Joe";** Click Save.*

Special Note: *In the examples above "All State Teachers" is not a group, it is actually a mailbox. Thus it does not contain actual users and should NOT be treated, as normal security groups would be.*



* Display name: Harrison Co Teachers

* E-mail address: ahct @ harrison.kyschools.us

Description:

By default, only senders inside your organization can send messages to this group. To allow someone outside your organization to send to the group, contact your helpdesk. To restrict the senders inside your organization who can send to the group, add users or groups to the list below. If you do this, mail sent by anyone else will be rejected.

- Admin TDL
- All State Teachers
- Harrison Co Board Members
- Harrison Co Personnel

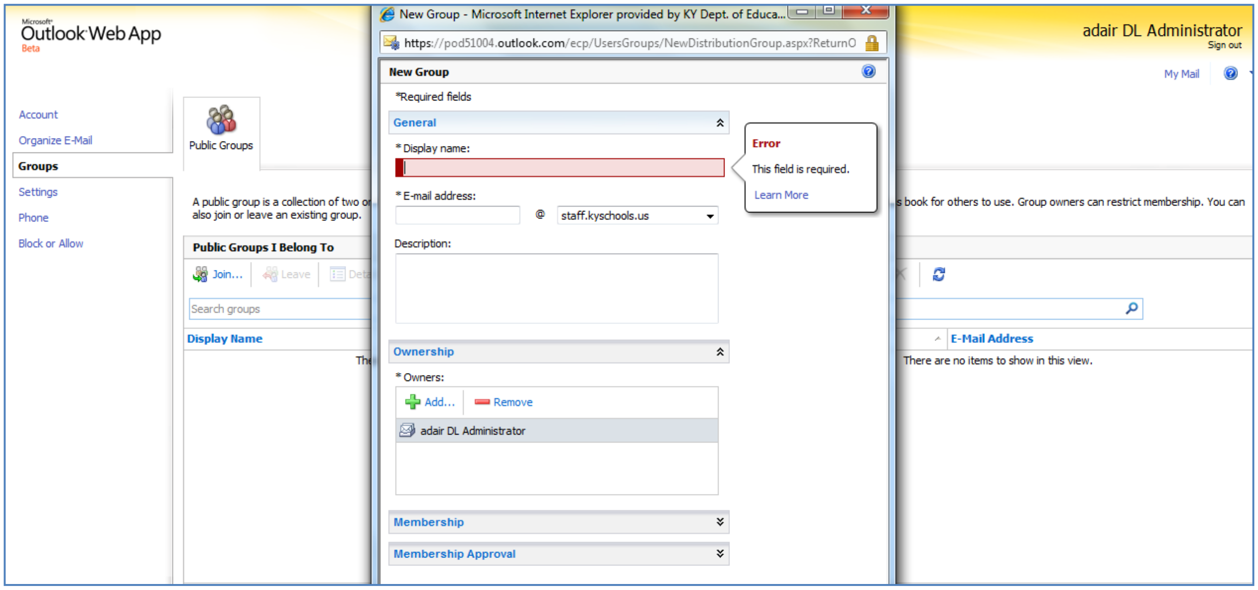
3.1.5.3 Renaming a Security or Distribution Group in Active Directory

If a Security or Distribution Group is being managed from Active Directory and the desire is to rename the group; highlight the group in ADUC > hit F2 > and type desired name. This change will not change the SMTP address of the group.

3.1.5.4 User Created Shared Distribution Groups

End users have the ability to create Staff Distribution Groups, which would be seen by all staff members in the state. This is a new feature that has not been available in previous versions of the KETS Exchange System. As stated in the section entitled *Naming of Object and GAL Visibility* it's important that end users understand good naming standards. From OWA, a user would select 'Options' from the top right of the screen which would result in the screen below which is in the background. They would then select 'Groups' as shown below. They would then select *New* from the right pane which would result in the active window you see below. *Note: Students cannot create publicly shared DGs.*

***Important Note:** When a Staff user creates a Distribution Group a message is sent to members of the Notifications@district.kyschools.us DG. This gives districts the ability to act upon these groups if they feel the need, either to delete user created groups, verify naming standardization, etc*



https://pod51004.outlook.com/ecp/UsersGroups/NewDistributionGroup.aspx?ReturnO

A public group is a collection of two o... also join or leave an existing group. ...s book for others to use. Group owners can restrict membership. You can

There are no items to show in this view.

*Required fields

* Display name:

Error

This field is required.

Learn More

* E-mail address: @ staff.kyschools.us

Description:

* Owners: adair DL Administrator

3.1.5.5 Student - Distribution Group Administration

Districts have the ability to create Distribution Groups in the Student Tenant (GAL) through use of the DLAdmin@stu.district.kyschools.us account. These DGs can be set as visible in the GAL (default) or hidden. Districts may choose to create hidden DGs so students would not see these in their GAL, but allow staff members to send to the SMTP address of the DG (or a contact created in the Staff Tenant). The DG could be moderated or locked-down as to who could send.

Note: It's important to reiterate that a DG, by default, is set as 'visible' in the Student GAL. This is important to understand as any student in any district would, by default, have the ability to see and send to this DG.

Student DGs *cannot* be created using ADUC. Groups or DGs created in ADUC are *not* synced to the Student Tenant so they must be created/managed by the Exchange Control Panel or Remote PowerShell. Use the information provided in the *Staff – Distribution Group Administration* section for using the Exchange Control Panel above to create/manage the DGs in the Student Tenant.

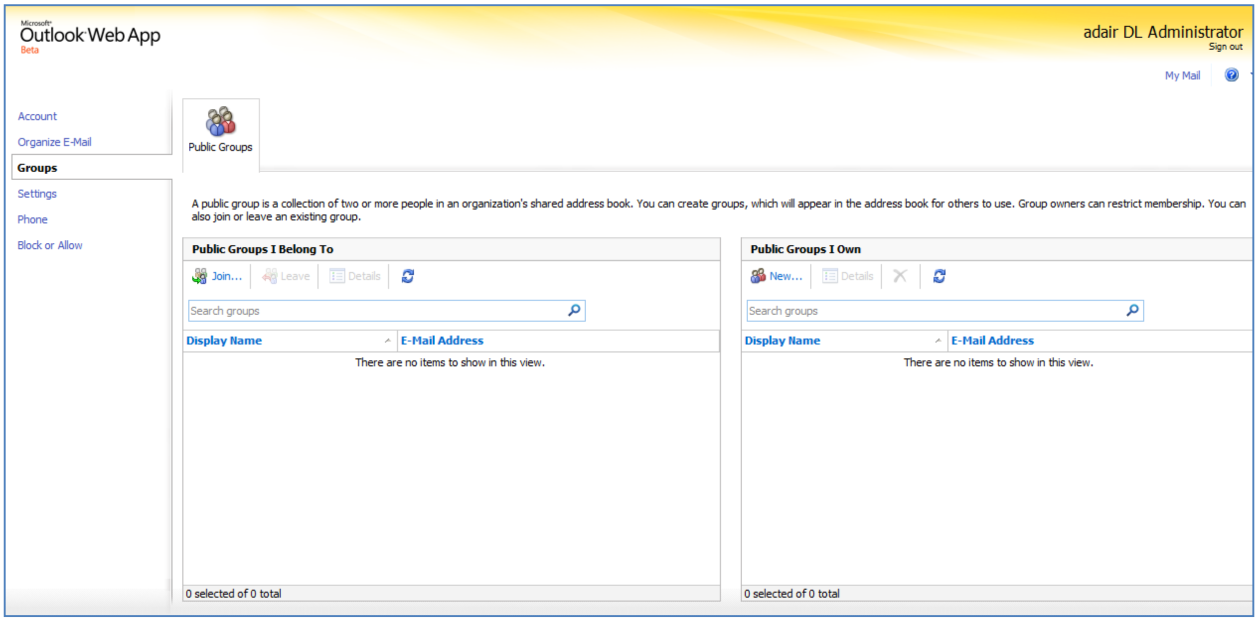
3.1.5.6 everyoneDL Distribution Group

A Dynamic Distribution Group exists for both the Staff and Students for each district. Since these are Dynamic DGs they will automatically add membership for any users that are created, so no one has to manually add membership to these groups. These are hidden DGs, meaning they will not show in the Global Address List. Users within a district can send to these by typing the SMTP address of the DGs (everoneDL@district.kyschools.us to send to all Staff in a district or everyoneDL@stu.district.kyschools.us to send to all students in a district). A contact could be created in the Staff GAL which would point to the student's EveryoneDL if desired.

There is a 'moderator' set on each of these distribution groups, meaning that any message which is sent to the SMTP address of the DG would first be sent to a 'moderator'. This person would have to 'allow' or 'reject' any message send to either of these groups. You can also select specific users whose messages do not have to go through a moderator. The account that is set as the moderator is DLAdmin@district.kyschools.us for the Staff DG and DLAdmin@stu.*district*.kyschools.us for the Student DG (ex. DLAdmin@stu.woodford.kyschools.us). A designated person in the district would need to either login to OWA/Outlook using this account to check for moderated messages sent to the DG, or setup an Inbox Rule to forward the mail to another mailbox. If 'forwarding' was set in the DLAdmin mailbox, the mailbox forwarded to would get the message, but they would have to in turn log in to the DLAdmin account to approve of the message and allow sending.

Note: The DLAdmin account also has permissions to create/administer additional DGs in the Student Tenant if desired.

To access the group modification area in OWA log in using https://outlook.com. Choose 'Options' to reveal the menus shown below.



A public group is a collection of two or more people in an organization's shared address book. You can create groups, which will appear in the address book for others to use. Group owners can restrict membership. You can also join or leave an existing group.

There are no items to show in this view.

0 selected of 0 total

There are no items to show in this view.

0 selected of 0 total

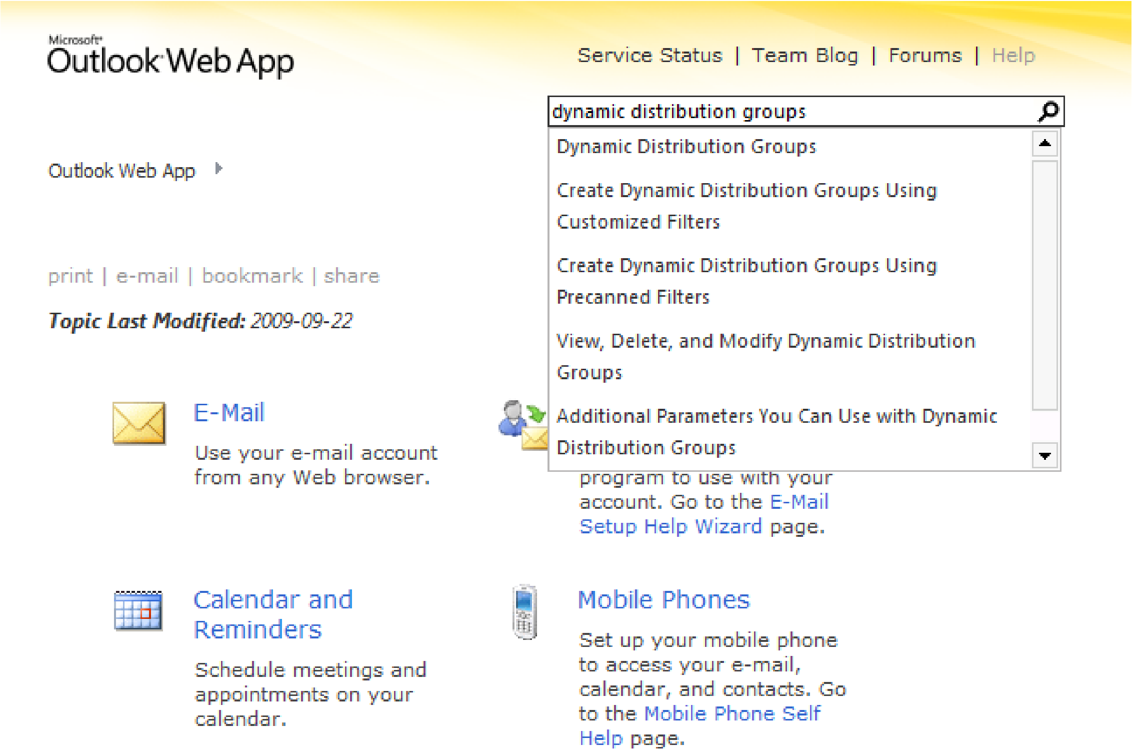
3.1.5.7 Dynamic Distribution Groups

Outlook Live supports a special kind of distribution group called a Dynamic Distribution Group. District IT Administrators have the ability to create Dynamic Distribution Groups (DDGs) for either Staff or Students. Unlike the static membership list of a regular distribution group, also known as a *public group*, the membership list for a dynamic distribution group is calculated every time a message is sent to the group. This calculation is based on filters and conditions you define when you create the group. When an e-mail message is sent to a dynamic distribution group, it is delivered to all recipients in the organization that match the filters and conditions you defined. This can be triggered off of a number of attributes of user objects.

Only the respective OutlookAdmin account has access to create DDGs. Dynamic Distribution Groups can only be created using Windows PowerShell and a proper email address must be specified upon creation.

For reference when creating a new DDG, see the PowerShell Examples section.

For more information on how to create DDGs please search http://www.help.outlook.com for 'Dynamic Distribution Groups'.

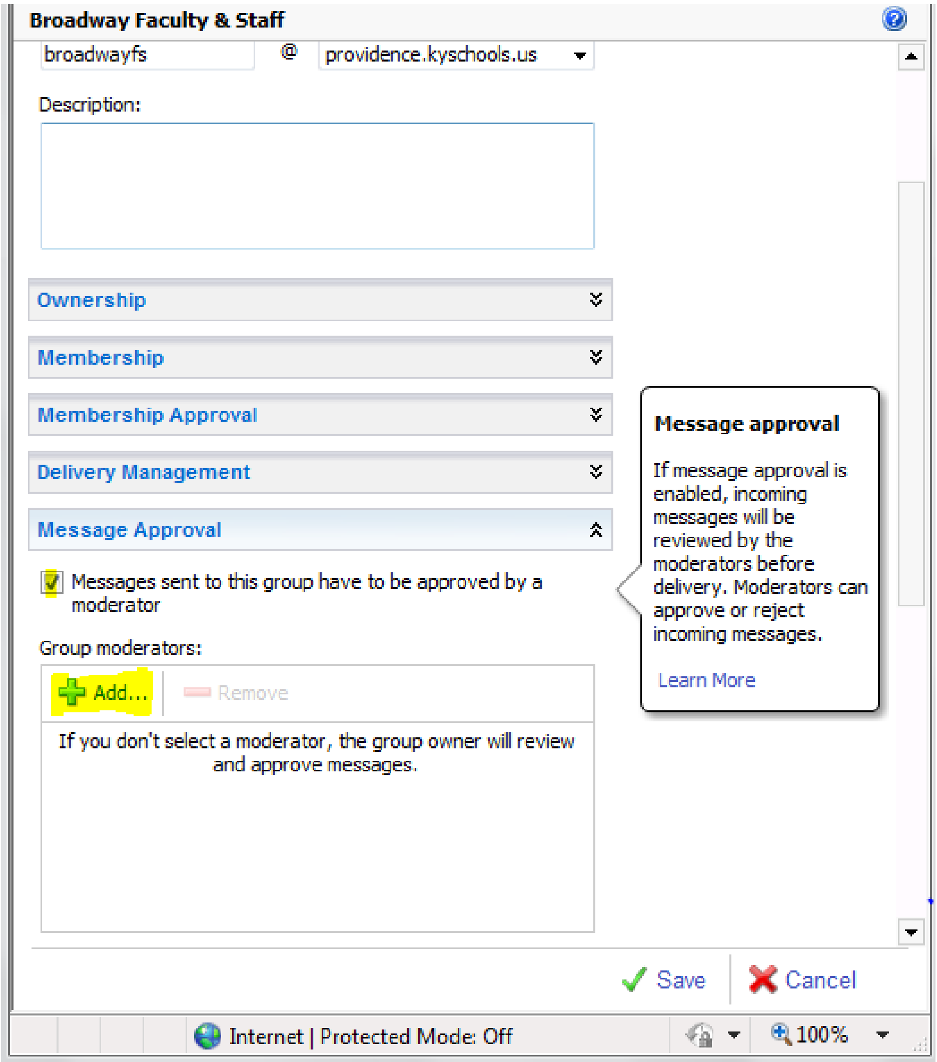


Microsoft Outlook Web App
Service Status | Team Blog | Forums | Help
dynamic distribution groups
Dynamic Distribution Groups
Create Dynamic Distribution Groups Using Customized Filters
Create Dynamic Distribution Groups Using Precanned Filters
View, Delete, and Modify Dynamic Distribution Groups
Additional Parameters You Can Use with Dynamic Distribution Groups
Outlook Web App
print | e-mail | bookmark | share
Topic Last Modified: 2009-09-22
E-Mail
Use your e-mail account from any Web browser.
program to use with your account. Go to the E-Mail Setup Help Wizard page.
Calendar and Reminders
Schedule meetings and appointments on your calendar.
Mobile Phones
Set up your mobile phone to access your e-mail, calendar, and contacts. Go to the Mobile Phone Self Help page.

3.1.5.8 Sending to Large Groups

Large Distribution Groups (those with membership larger than 500) or Dynamic Distribution Groups should be set with Moderation (**http://help.outlook.com/en-us/140/cc498696.aspx?sl=1**). Also when sending to large Distribution Groups users should always send to the group using the BCC (Blind Carbon Copy) option on the New Mail form. This would normally be district administrative staff that should have access to send to larger groups (membership of 500 or more). A good practice is to choose themselves in the To: field or another predefined mailbox for this purpose. By sending to the BCC you take away the potential for recipients of a message to a large group to hit 'Reply All', as objects on the BCC are not included on a 'Reply All'.

Any distribution Groups that have large membership (ex. Providence Teachers) should be moderated. This means that any messages sent to the Distribution Group would first go to a mailbox designated to approve messages that are sent. This limits the amount of unnecessary messages that are sent to large numbers of recipients. This can be done from within OWA logged in as DLAdmin (or by any Owner of that group).



☑ Messages sent to this group have to be approved by a moderator

If you don't select a moderator, the group owner will review and approve messages.

Message approval

If message approval is enabled, incoming messages will be reviewed by the moderators before delivery. Moderators can approve or reject incoming messages.

3.1.5.9 Creating Contacts

Contacts can be created in ADUC for the Staff Tenant but not the Student Tenant. Contacts are only provisioned at night from AD to Outlook Live. Create contacts in any OU under Leadership or Staff (other than _Groups). Most districts utilize the _Exchange Resources OU under Staff for Contact creation. You must specify the SMTP address of the contact.

3.1.6 KETS Specific Attributes and Active Directory Attribute flow

There are additional attributes that are ‘KETS specific’ attributes, some created for district use and others utilized by OLPS for provisioning. There are three new tabs in Active Directory Users in Computers; *KETS EDU, KETS Custom* and *Attribute Editor.* The *Attribute Editor* tab is part of the default ADUC console, but is only available when viewing ‘Advanced Features’. The *KETS EDU* and *KETS Custom* tabs are available after installing an msi which will reveal these tabs in ADUC on an administrator’s workstation.

* * The installer for ADUC to show these additional tabs can be found at http://education.ky.gov/districts/tech/tss/Pages/default.aspx > then select (KETS Email Services) and (Install Files).

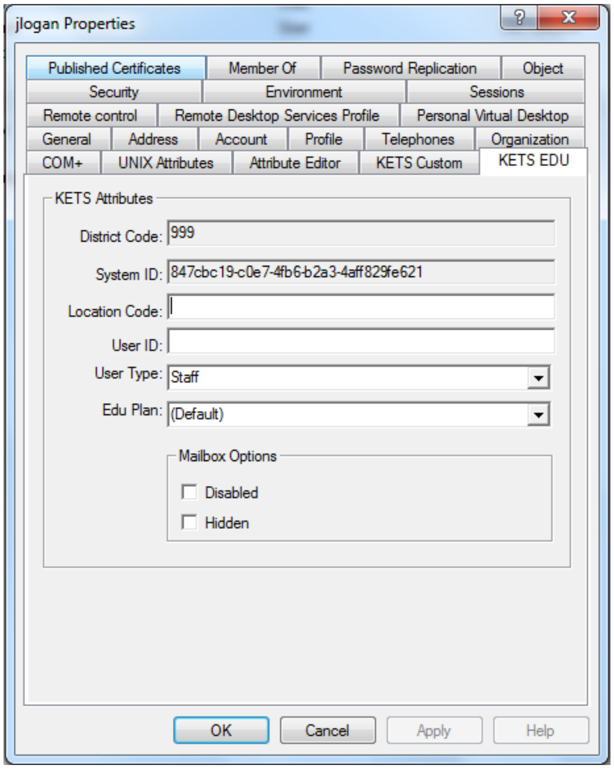
Note: The 32-bit version (KETSEdu_ADUC_32bit.msi) is for any 32-bit OS. The 64-bit version (KETSEdu_ADUC_64bit.msi) works for Windows Server 2008 64-bit and Windows 7 64-bit. 64-bit operating systems other than those specified will not show the 'Attribute Editor' tab. The 'Attribute Editor' tab (available with the Microsoft Remote Server Administration Tools (RSAT)) is to be used to read/modify the extensionAttibutes (aka Custom Attributes). These are attributes that were part of the legacy Exchange 2003 system which some districts chose to utilize. PLEASE be cautious while in Attribute Editor as IT Admins have the permission to modify many of the Active Directory attributes while in this tab, which could cause ill effect. It's also important to note that districts have 15 additional attributes (ketsCustom1 – ketsCustom15) that can be used as the district sees fit. These are explained later in the sections entitled 'KETS Specific Attributes and Active Directory Attribute Flows'.

Important Note: *If you have installed the above stated apps and still do not see the Attribute Editor tab you should create a shortcut on your desktop with the following:*

```
%SystemRoot%\System32\mmc.exe -32 %SystemRoot%\system32\dsa.msc
```

The -32 switch should display the Attribute Editor tab

These new attributes need to be discussed as district administrators should understand what each is used for. Administrators also can leverage these values for programming, LDAP queries, etc. against Active Directory. These attributes are visible and modifiable on either the *KETS EDU* or *Attribute Editor*, but it is highly recommended to use the *KETS EDU* tab. A description of the attributes and mappings are provided in the following sections, though a more in-depth discussion can be found in the section entitled *Active Directory* in Section 3 above



KETS Attributes

District Code: 999

System ID: 847cbc19-c0e7-4fb6-b2a3-4aff829fe621

Location Code:

User ID:

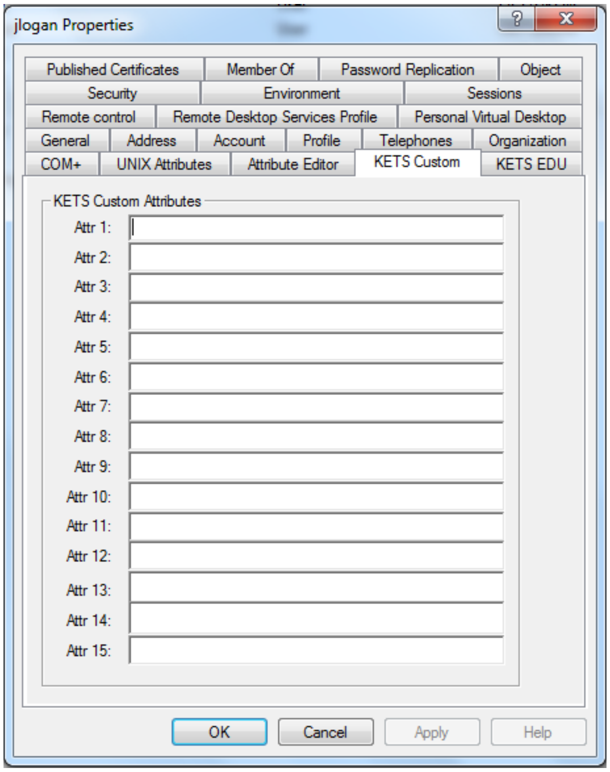
User Type: Staff

Edu Plan: (Default)

Mailbox Options

☐ Disabled

☐ Hidden



KETS Custom Attributes

Attr 1:
Attr 2:
Attr 3:
Attr 4:
Attr 5:
Attr 6:
Attr 7:
Attr 8:
Attr 9:
Attr 10:
Attr 11:
Attr 12:
Attr 13:
Attr 14:
Attr 15:

3.1.6.1.1 OLPS Provisioned Attributes (KETS EDU Tab in ADUC)

The attributes shown on the *KETS EDU* tab are mapped to Active Directory LDAP attributes. The following two attributes are set by the system. They are explained here so that districts can leverage these attributes, not to modify their values.

Note: These attributes are NOT to be populated or modified by the district. Modifying these values can render undesirable results.

ketsDistrictCode

Purpose: Value relates to three-digit district number
Flows to *extensionAttribute14* and *ketsDistrictCode* in Active Directory
Flows to *CustomAttribute1* in Outlook Live
Used to set '*Company*' attribute in Outlook Live – The district name (ex. 'providence') is set in the Company field for mailboxes in Outlook Live

ketsEduSystemID

Purpose: Immutable ID created by OLPS for uniqueness, used to create Windows Live ID
Flows to *Name (CN)* in Outlook Live

3.1.6.1.2 District Modified Attributes

The objects listed below are populated directly, some indirectly, by the district either by OU placement, choices on the *KETS EDU* or through batch modification.

Note: Do NOT populate or modify these attributes without a complete understanding of the valid values and their results.

ketsEduDisable

Purpose: Disables access to mailbox in Outlook Live (Outlook Live)

Note: Mailbox will continue to receive mail

Values: TRUE or FALSE

Default: **FALSE**

Flows to *CAS Mailbox Settings* in Outlook Live

Note: If this is done through the KETS EDU tab in ADUC it can take up to two hours to go through the OLPS system. This task can be performed with higher priority through the KETS Control Panel for administrators (discussed in the next section).

ketsEduHidden

Purpose: Hides visibility in Outlook Live Global Address List

Values: TRUE or FALSE

Default: **FALSE**

ketsEduPlan

Purpose: Determines if system is to create a mailbox for the specified user

Values: <default> or NoMail

Default: ***<default>*** *which results in Mailbox creation*

Note: If not populated a mailbox will be created for the user

ketsUserType

Purpose: To classify user type

Values: STAFF, STUDENT or RESOURCE

Note: Objects set to 'Resource' are not provisioned by OLPS

Default: <not set>

Note: If left blank will be populated by OU placement of object

Results in placement of mailbox in correct GAL

Flows to *extensionAttribute15* in Active Directory

ketsLocationCode

Purpose: Location Identifier

Value: Entered by district

Default: <not set>

Flows to *customAttribute2* at Outlook Live

ketsUserID

Purpose: System Attribute (do not assign)

ketsCustom1 through ***ketsCustom15***

Purpose: For district population and use
Does not flow to Outlook Live

Note: The ketsCustom attributes were created solely for district use at their discretion.

3.1.6.1.3 Synced Attributes between Active Directory and Outlook Live

The list below contains the Active Directory attributes that are being synchronized to the corresponding Outlook Live objects. These can be leveraged by the district for Exchange Web Services programming, Remote PowerShell, Dynamic Distribution Group creation, etc.

The flow is from Active Directory object attribute to Outlook Live object attribute.

*Note: The '**Company**' attribute in Outlook Live is populated with the district name (ex. 'providence'). This is regardless of the value in AD for a user, as the value of 'Company' does not 'flow' from AD to Outlook Live.*

Mailboxes, MailUsers & MailContacts

```
<Map Source="ketsSystemID" Destination="Name" Macro="" />
<Map Source="ObjectID" Destination="DirSyncId" Macro="" />
<Map Source="ketsEduDisable" Destination="AccountDisabled" Macro="" />
<Map Source="ketsEduHidden" Destination="AccountHidden" Macro="" />
<Map Source="mail" Destination="EmailAddress" Macro="" />
<Map Source="l" Destination="City" Macro="" />
<Map Source="ketsDistrictCode" Destination="CustomAttribute1" Macro="" />
<Map Source="ketsLocationCode" Destination="CustomAttribute2" Macro="" />
<Map Source="department" Destination="Department" Macro="" />
<Map Source="displayName" Destination="DisplayName" Macro="" />
<Map Source="facsimileTelephoneNumber" Destination="Fax" Macro="" />
<Map Source="givenName" Destination="FirstName" Macro="" />
<Map Source="homePhone" Destination="HomePhone" Macro="" />
<Map Source="initials" Destination="Initials" Macro="" />
<Map Source="sn" Destination="LastName" Macro="" />
<Map Source="mobile" Destination="MobilePhone" Macro="" />
<Map Source="info" Destination="Notes" Macro="" />
<Map Source="physicalDeliveryOfficeName" Destination="Office" Macro="" />
<Map Source="pager" Destination="Pager" Macro="" />
<Map Source="telephoneNumber" Destination="Phone" Macro="" />
<Map Source="postalCode" Destination="PostalCode" Macro="" />
<Map Source="st" Destination="StateOrProvince" Macro="" />
<Map Source="streetAddress" Destination="StreetAddress" Macro="" />
<Map Source="title" Destination="Title" Macro="" />
```

3.1.7 KETS Control Panel and Object Provisioning

The KETS Control Panel is a customized web interface for administrative control and utilities that are specific to KETS needs. This is not to be confused with the Exchange Control Panel (https://outlook.com/ecp) which is the Microsoft default portal for management of Outlook Live and its components (primarily Distribution Group management for Staff, and Tenant management for Students).

While ADUC (Active Directory Users and Computers) and ECP (Exchange Control Panel) will continue to be administrative tools for most tasks there are a few administrative functions that can only be performed in the KETS Control Panel. There are two different views to the KETS Control Panels, one for administrators and one for users. The differences between these different portal views are discussed in the following sections.

Different object types (user, group, contact) that are created in Active Directory are provisioned to Outlook Live on different schedules. Those schedules are listed below.

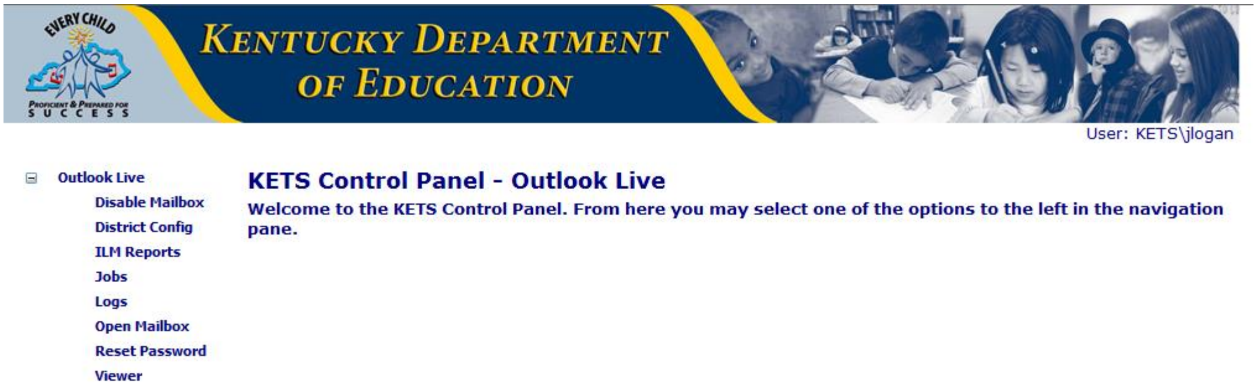
Staff User objects	-	every 15 minutes, with replication latency could be up to 1 hour
Student User objects	-	every 6 hours
Groups	-	nightly
Contacts	-	nightly

Note: User object deletions only provision at night. This is an important note as if the desire upon deletion is that the user cannot get into mail (disciplinary issues, etc) you must also go to the KETS Control Panel and Disable the mailbox so they cannot access open the mailbox.

Districts and run manual provisioning jobs using the KETS Control Panel (explained below) for user objects. This will not affect groups or contacts which run one during the night. This means that groups and contacts created in AD will not show in the Global Address List until the following day.

3.1.7.1 KETS Control Panel – Administrative Tasks

Members of the *DIST Support Admins, DIST Staff User Admins, DIST Student User Admins, DIST Staff All Mailbox Access* or *DIST Student All Mailbox Access* will have authority in the admin section of the KETS Control Panel to modify settings. The URL again is https://live.kyschools.us/admin

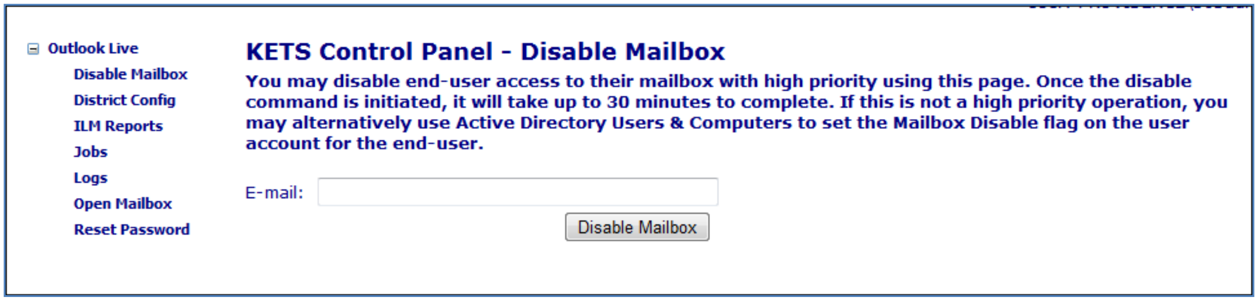


KETS Control Panel - Outlook Live

Welcome to the KETS Control Panel. From here you may select one of the options to the left in the navigation pane.

3.1.7.1.1 Disable Mailbox

Members of *DIST Support Admins, DIST Staff User Admins* or *DIST Student User Admins* are able to disable end-user access to their mailbox using this page. *DIST Support Admins* can disable any mailbox, where as *DIST Staff User Admins* can only reset user passwords (likewise for *DIST Student User Admins*). Once the disable command is initiated it may take a few minutes to complete. If this is not a high priority operation you may alternatively use Active Directory Users & Computers to set the Mailbox Disable flag on the user account for the end-user.



KETS Control Panel - Disable Mailbox

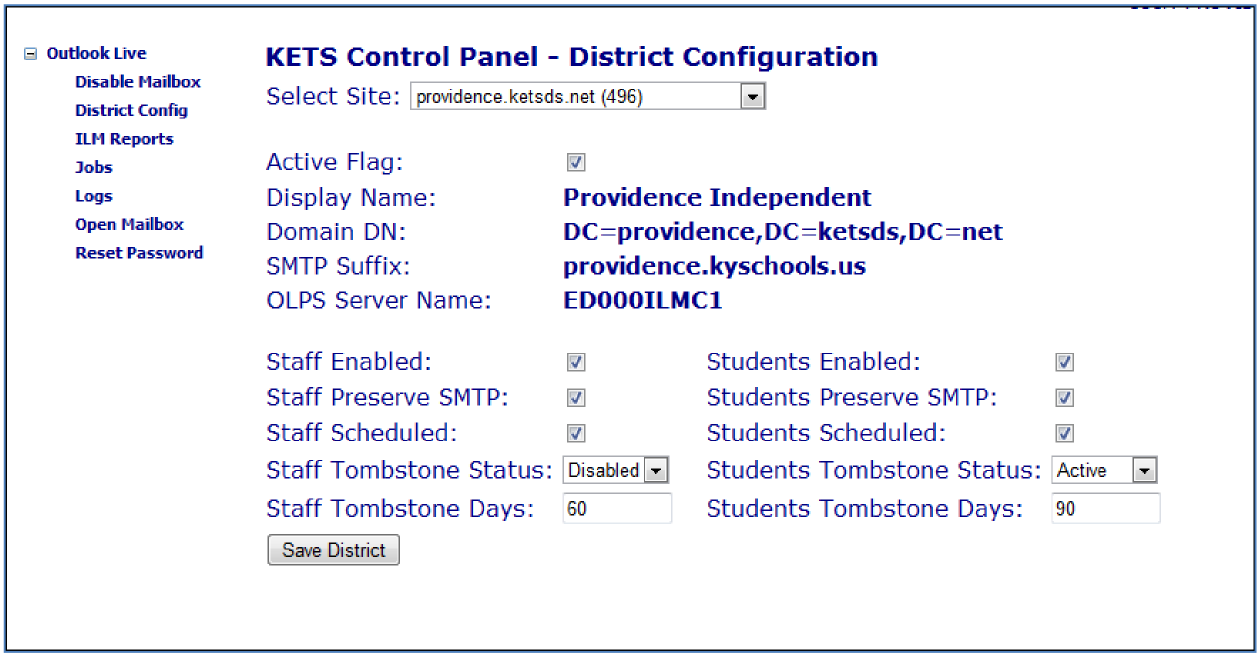
You may disable end-user access to their mailbox with high priority using this page. Once the disable command is initiated, it will take up to 30 minutes to complete. If this is not a high priority operation, you may alternatively use Active Directory Users & Computers to set the Mailbox Disable flag on the user account for the end-user.

E-mail:

Very Important Note: Disabling a mailbox, regardless of how, as well as deleting the AD object will NOT restrict access to the other Live services (Skydrive, Spaces, etc).

3.1.7.1.2 District Config

The District Config area of the KETS Control Panel is where members of the DIST Support Admins group have access to modify certain settings of provisioning. Start by selecting the appropriate domain from the *Select Site* dropdown. Some of the settings are unavailable ('grayed' out) as they can cause dramatic ill-affects if not handled properly. A change to any of these values will only be applied on the weekend, so the expectation should be modifications will be implemented by the following Monday.



KETS Control Panel - District Configuration

Select Site: providence.ketsds.net (496)

Active Flag: ☑

Display Name: Providence Independent

Domain DN: DC=providence,DC=ketsds,DC=net

SMTP Suffix: providence.kyschools.us

OLPS Server Name: ED000ILMC1

Staff Enabled: ☑ Students Enabled: ☑

Staff Preserve SMTP: ☑ Students Preserve SMTP: ☑

Staff Scheduled: ☑ Students Scheduled: ☑

Staff Tombstone Status: Disabled Students Tombstone Status: Active

Staff Tombstone Days: 60 Students Tombstone Days: 90

The defaults are shown above.

- **Staff Scheduled / Students Scheduled**
  - If checked sets provisioning to run on a schedule for either Staff or Students
    - **Default if checked, 15 minutes for Staff and 6 hours for Students**
      Note: Staff provisioning is set to 'kick off' every 15 minutes, though it could take up to an hour depending on the AD replication interval.
  - If unchecked would disable automatic runs of provisioning. This would allow for a district to make mass modifications/etc and/or run provisioning manually (utilizing the 'Jobs' option explained below)
- **Staff Tombstone Status / Student Tombstone Status**
  - If set to Active, will allow user to access e-mail (Outlook 2007 and Outlook.com only, not mail.kyschools.us) after Active Directory account is deleted, for a period up to the 'Staff/Student Tombstone Days' value
  - If set to Disabled, restricts user access to e-mail after Active Directory user object deletion for a period up to the 'Staff/Student Tombstone Days' value

    Notice in the above screenshot which shows the defaults, Staff are set to 'Disabled' which means that if the user object is deleted in AD the user could not login to the mailbox. The mailbox could, for 60 days as the default is set, be reattached to the User object in AD. This process is explained elsewhere in this document.
    Very Important Note: If a student AD object is deleted the student could still login and access e-mail if the 'Student Tombstone Status is left as 'Active'. If the desire on an individual basis it to both delete the AD account and the mailbox set the Edu Plan to 'NoMail' on the KETS EDU tab in ADUC. Allow this to filter through the system then delete the AD account. If the desire is always to delete the mailbox and the Windows Live ID the Tombstone Status could be set to Disabled and Tombstone Days set to a shorter

period. It's important to leave some period of time as this can allow for reattaching mailboxes to deleted AD object in case of mistaken deletes.

- **Staff Tombstone Days / Student Tombstone Days**
  - Sets the number of days after an Active Directory user object is deleted until the corresponding mailbox is deleted

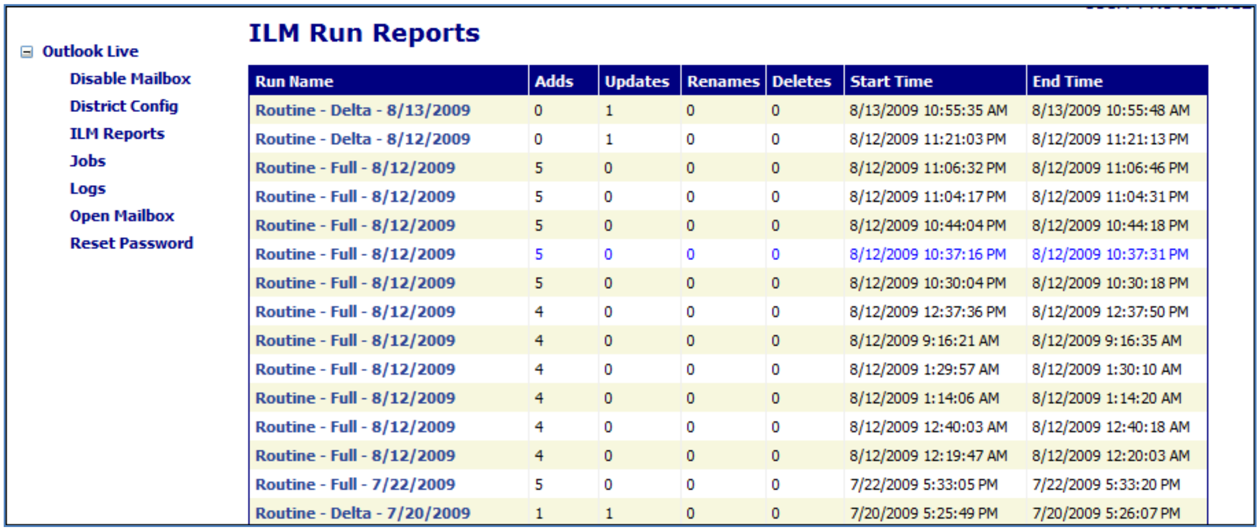
The process of 'Tombstoning' simply means a period of time in which a mailbox could still be accessed and/or reattached after the corresponding Active Directory user object is deleted. If, for instance, the Staff Tombstone Days are set to 60 days and an AD user account is deleted the corresponding Outlook Live mailbox would stay accessible for that user, assuming 'Tombstone Status' is set to *Active*. ***After the 'Tombstone Days' have passed the mailbox will be deleted, as well as the Windows Live ID and all tools and content associated with that Live ID.***

To reattach a deleted user object to a mailbox:
If, during the 'Staff Tombstone Days' period, the desire was to recreate the AD user object and reattach it to the mailbox the district would have to create the user object and assign the 'E-mail' attribute the value of the SMTP address. This MUST be done immediately after user creation. This means that the desired user's AD object would need to be recreated in ADUC, then immediately after the creation double-click on the user object and add the user's original SMTP address in the *E-mail* field on the 'General' tab. This will trigger the provisioning system to find the 'tombstoned' Live ID and link it to the new user.

***VERY IMPORTANT Note**: It is extremely important the districts understand these settings before changing them. 'Playing' with Tombstone settings can cause undesirable affects.*

3.1.7.1.3 ILM Reports

Displays the OLPS provisioning runs. You can click on each Run Name to get more information. This is used for troubleshooting.



ILM Run Reports

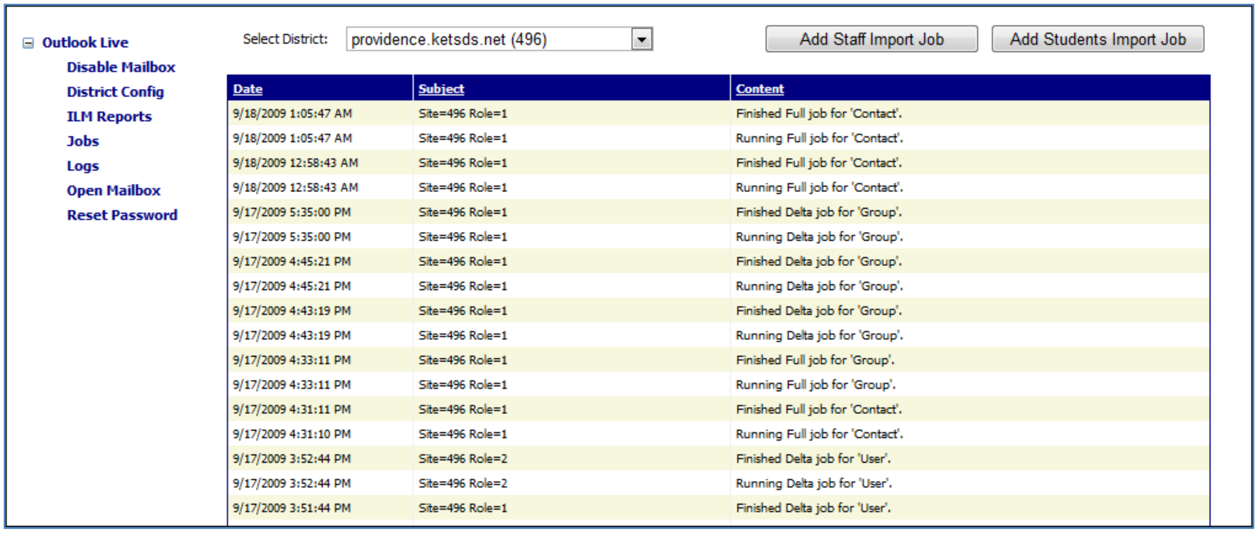
Run Name	Adds	Updates	Renames	Deletes	Start Time	End Time
Routine - Delta - 8/13/2009	0	1	0	0	8/13/2009 10:55:35 AM	8/13/2009 10:55:48 AM
Routine - Delta - 8/12/2009	0	1	0	0	8/12/2009 11:21:03 PM	8/12/2009 11:21:13 PM
Routine - Full - 8/12/2009	5	0	0	0	8/12/2009 11:06:32 PM	8/12/2009 11:06:46 PM
Routine - Full - 8/12/2009	5	0	0	0	8/12/2009 11:04:17 PM	8/12/2009 11:04:31 PM
Routine - Full - 8/12/2009	5	0	0	0	8/12/2009 10:44:04 PM	8/12/2009 10:44:18 PM
Routine - Full - 8/12/2009	5	0	0	0	8/12/2009 10:37:16 PM	8/12/2009 10:37:31 PM
Routine - Full - 8/12/2009	5	0	0	0	8/12/2009 10:30:04 PM	8/12/2009 10:30:18 PM
Routine - Full - 8/12/2009	4	0	0	0	8/12/2009 12:37:36 PM	8/12/2009 12:37:50 PM
Routine - Full - 8/12/2009	4	0	0	0	8/12/2009 9:16:21 AM	8/12/2009 9:16:35 AM
Routine - Full - 8/12/2009	4	0	0	0	8/12/2009 1:29:57 AM	8/12/2009 1:30:10 AM
Routine - Full - 8/12/2009	4	0	0	0	8/12/2009 1:14:06 AM	8/12/2009 1:14:20 AM
Routine - Full - 8/12/2009	4	0	0	0	8/12/2009 12:40:03 AM	8/12/2009 12:40:18 AM
Routine - Full - 8/12/2009	4	0	0	0	8/12/2009 12:19:47 AM	8/12/2009 12:20:03 AM
Routine - Full - 7/22/2009	5	0	0	0	7/22/2009 5:33:05 PM	7/22/2009 5:33:20 PM
Routine - Delta - 7/20/2009	1	1	0	0	7/20/2009 5:25:49 PM	7/20/2009 5:26:07 PM

3.1.7.1.4 Jobs

The ‘Jobs’ selection allows for a manual run of OLPS provisioning, meaning you can force a run for ‘User mailbox provisioning’ for either Staff or Students.   Selecting one of these options would take any new/modified user objects (either Staff or Students) and create/modify Windows Live IDs and the corresponding mailboxes for those objects. This would also ‘write back’ to the Active Directory user objects, modifying the E-mail Address and UPN for logon as SMTP. You can also see the history of all jobs run in the OPLS system for a given district.

Realize that an import job runs every 15 minutes on a schedule by default for Staff and 6 hours for Students (staff could take up to an hour with replication latencies). The ability to run a manual job could be helpful, for instance if districts did not want to wait 6 hours for Student provisioning.   This can work in conjunction with ‘Staff / Student Scheduled’ under the *District Config* option explained above, where you *could* turn off provisioning as a schedule and choose to manually run jobs. It’s important to note, however, that groups and contacts from Active Directory do not adhere to the manual job runs, meaning that if either ‘Add Staff Import Job’ or Add Student Import Job’ is chosen this only affects user objects in AD which require mailbox access.

To kick off a run of OLPS provisioning you would either click “Add Staff Import Job” or “Add Student Import Job” respectively.



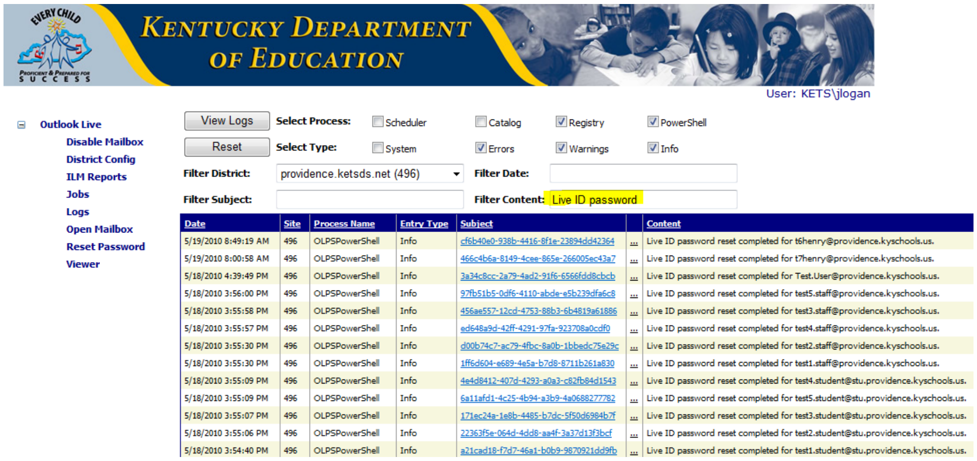
Select District: providence.ketsds.net (496)

Date	Subject	Content
9/18/2009 1:05:47 AM	Site=496 Role=1	Finished Full job for 'Contact'.
9/18/2009 1:05:47 AM	Site=496 Role=1	Running Full job for 'Contact'.
9/18/2009 12:58:43 AM	Site=496 Role=1	Finished Full job for 'Contact'.
9/18/2009 12:58:43 AM	Site=496 Role=1	Running Full job for 'Contact'.
9/17/2009 5:35:00 PM	Site=496 Role=1	Finished Delta job for 'Group'.
9/17/2009 5:35:00 PM	Site=496 Role=1	Running Delta job for 'Group'.
9/17/2009 4:45:21 PM	Site=496 Role=1	Finished Delta job for 'Group'.
9/17/2009 4:45:21 PM	Site=496 Role=1	Running Delta job for 'Group'.
9/17/2009 4:43:19 PM	Site=496 Role=1	Finished Delta job for 'Group'.
9/17/2009 4:43:19 PM	Site=496 Role=1	Running Delta job for 'Group'.
9/17/2009 4:33:11 PM	Site=496 Role=1	Finished Full job for 'Group'.
9/17/2009 4:33:11 PM	Site=496 Role=1	Running Full job for 'Group'.
9/17/2009 4:31:11 PM	Site=496 Role=1	Finished Full job for 'Contact'.
9/17/2009 4:31:10 PM	Site=496 Role=1	Running Full job for 'Contact'.
9/17/2009 3:52:44 PM	Site=496 Role=2	Finished Delta job for 'User'.
9/17/2009 3:52:44 PM	Site=496 Role=2	Running Delta job for 'User'.
9/17/2009 3:51:44 PM	Site=496 Role=1	Finished Delta job for 'User'.

Note: Active Directory replication has to complete for a given user for OLPS to pick the change up. OLPS is reading/writing from Domain Controllers (one from each district domain) which resides at KIDS. Active Directory replication is set to 60 minutes between sites, so it could take ‘up to’ 1 hour depending on the replication windows for a creation/modification/deletion to replicate so that OLPS will see the change.

3.1.7.1.5 Logs

Displays logs for multiple components of OLPS. IT Admins can utilize this for troubleshooting. You can search using ‘Filter Subject’ for SMTP Address, SAMAccountName, etc. Also, members of the *Notifications* Distribution Group would receive nightly notifications through e-mail. Districts should populate this group with members that wish to get information on successes, failures, etc involved with provisioning between Active Directory and Outlook Live. A great feature as shown below is the ability to first do a ‘View Logs’ for the domain, then when you find a specific bit of information that you’re looking for, you can past it into the ‘Filter Content’ box to get only those types of events.



Select Process: □ Scheduler □ Catalog ☑ Registry ☑ PowerShell

Select Type: □ System ☑ Errors ☑ Warnings ☑ Info

Filter District: providence.ketsds.net (496)

Filter Date:

Filter Subject:

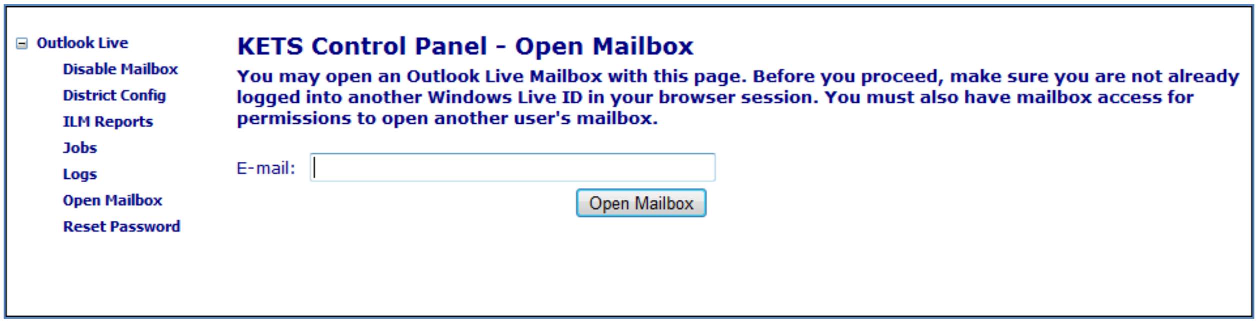
Filter Content: Live ID password

Date	Site	Process Name	Entry Type	Subject		Content
5/19/2010 8:49:19 AM	496	OLPSPowerShell	Info	cf6b40e0-938b-4416-8f1e-23894dd42364	...	Live ID password reset completed for t6henry@providence.kyschools.us.
5/19/2010 8:00:58 AM	496	OLPSPowerShell	Info	466c4b6a-8149-4cee-865e-266005ec43a7	...	Live ID password reset completed for t7henry@providence.kyschools.us.
5/18/2010 4:39:49 PM	496	OLPSPowerShell	Info	3a34c8cc-2a79-4ad2-91f6-6566fdd8cbcb	...	Live ID password reset completed for Test.User@providence.kyschools.us.
5/18/2010 3:56:00 PM	496	OLPSPowerShell	Info	97fb51b5-0df6-4110-abde-e5b239dfa6c8	...	Live ID password reset completed for test5.staff@providence.kyschools.us.
5/18/2010 3:55:58 PM	496	OLPSPowerShell	Info	456ae557-12cd-4753-88b3-6b4819a61886	...	Live ID password reset completed for test3.staff@providence.kyschools.us.
5/18/2010 3:55:57 PM	496	OLPSPowerShell	Info	ed648a9d-42ff-4291-97fa-923708a0cdf0	...	Live ID password reset completed for test4.staff@providence.kyschools.us.
5/18/2010 3:55:30 PM	496	OLPSPowerShell	Info	d00b74c7-ac79-4fbc-8a0b-1bbedc75e29c	...	Live ID password reset completed for test2.staff@providence.kyschools.us.
5/18/2010 3:55:30 PM	496	OLPSPowerShell	Info	1ff6d604-e689-4e5a-b7d8-8711b261a830	...	Live ID password reset completed for test1.staff@providence.kyschools.us.
5/18/2010 3:55:09 PM	496	OLPSPowerShell	Info	4e4d8412-407d-4293-a0a3-c82fb84d1543	...	Live ID password reset completed for test4.student@stu.providence.kyschools.us.
5/18/2010 3:55:09 PM	496	OLPSPowerShell	Info	6a11afd1-4c25-4b94-a3b9-4a0688277782	...	Live ID password reset completed for test5.student@stu.providence.kyschools.us.
5/18/2010 3:55:07 PM	496	OLPSPowerShell	Info	171ec24a-1e8b-4485-b7dc-5f50d6984b7f	...	Live ID password reset completed for test3.student@stu.providence.kyschools.us.
5/18/2010 3:55:06 PM	496	OLPSPowerShell	Info	22363f5e-064d-4dd8-aa4f-3a37d13f3bcf	...	Live ID password reset completed for test2.student@stu.providence.kyschools.us.
5/18/2010 3:54:40 PM	496	OLPSPowerShell	Info	a21cad18-f7d7-46a1-b0b9-9870921dd9fb	...	Live ID password reset completed for test1.student@stu.providence.kyschools.us.

3.1.7.1.6 Open Mailbox

Members of *DIST Staff All Mailbox Access* or *DIST Student All Mailbox Access* have permissions to open an Outlook Live Mailbox with this page. Type the SMTP address of the desired mailbox.

Note: Before you proceed make sure you are not already logged into another Windows Live ID in your browser session. Also, it is important to close all other browser windows before opening a mailbox.



KETS Control Panel - Open Mailbox

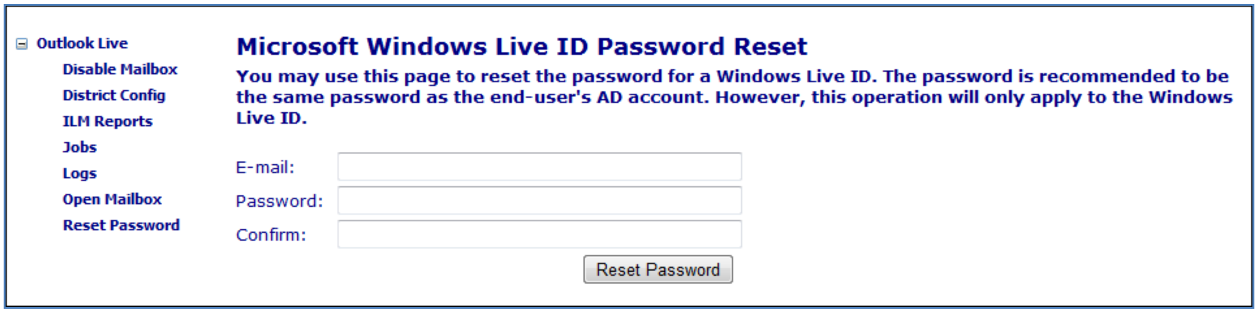
You may open an Outlook Live Mailbox with this page. Before you proceed, make sure you are not already logged into another Windows Live ID in your browser session. You must also have mailbox access for permissions to open another user's mailbox.

E-mail:

3.1.7.1.7 Reset Password

Members of *DIST Support Admins, DIST Staff User Admins* or *DIST Student User Admins* may use this page to reset the **password for a Windows Live ID only.** It does not impact the Active Directory account password. The password entered should match the end-user's Active Directory account password.

This is the same page that users will see if they utilize https://mail.kyschools.us/password.aspx



Microsoft Windows Live ID Password Reset

You may use this page to reset the password for a Windows Live ID. The password is recommended to be the same password as the end-user's AD account. However, this operation will only apply to the Windows Live ID.

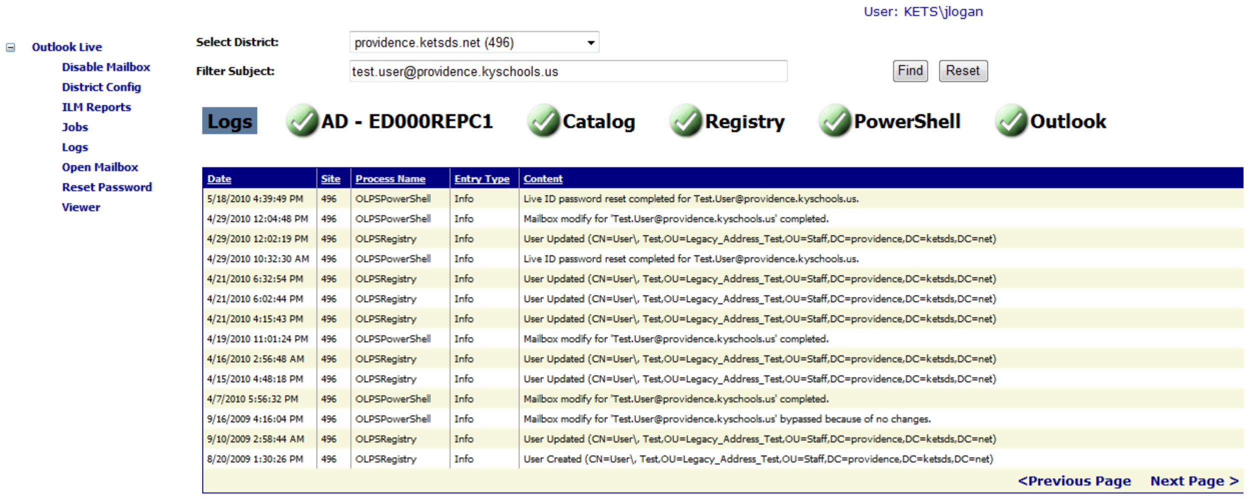
E-mail:

Password:

Confirm:

3.1.7.1.8 Viewer

By selecting Viewer on the left menu you can specify the SMTP address of a user and see each system the user is in. This will be mostly used by the Messaging and Directory Services team, KETS Service Desk, etc to troubleshoot Outlook Live provisioning issues, but it’s available if districts are interested.



Select District: providence.ketsds.net (496)

Filter Subject: test.user@providence.kyschools.us

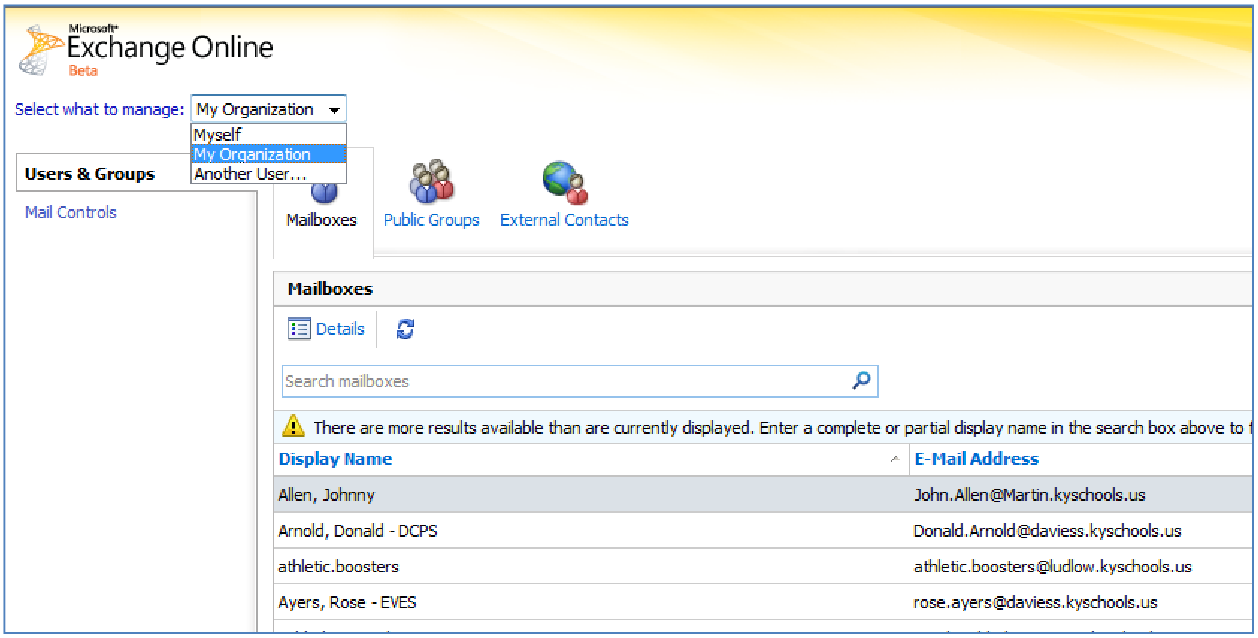
Date	Site	Process Name	Entry Type	Content
5/18/2010 4:39:49 PM	496	OLPSPowerShell	Info	Live ID password reset completed for Test.User@providence.kyschools.us.
4/29/2010 12:04:48 PM	496	OLPSPowerShell	Info	Mailbox modify for 'Test.User@providence.kyschools.us' completed.
4/29/2010 12:02:19 PM	496	OLPSRegistry	Info	User Updated (CN=User\, Test,OU=Legacy_Address_Test,OU=Staff,DC=providence,DC=ketsds,DC=net)
4/29/2010 10:32:30 AM	496	OLPSPowerShell	Info	Live ID password reset completed for Test.User@providence.kyschools.us.
4/21/2010 6:32:54 PM	496	OLPSRegistry	Info	User Updated (CN=User\, Test,OU=Legacy_Address_Test,OU=Staff,DC=providence,DC=ketsds,DC=net)
4/21/2010 6:02:44 PM	496	OLPSRegistry	Info	User Updated (CN=User\, Test,OU=Legacy_Address_Test,OU=Staff,DC=providence,DC=ketsds,DC=net)
4/21/2010 4:15:43 PM	496	OLPSRegistry	Info	User Updated (CN=User\, Test,OU=Legacy_Address_Test,OU=Staff,DC=providence,DC=ketsds,DC=net)
4/19/2010 11:01:24 PM	496	OLPSPowerShell	Info	Mailbox modify for 'Test.User@providence.kyschools.us' completed.
4/16/2010 2:56:48 AM	496	OLPSRegistry	Info	User Updated (CN=User\, Test,OU=Legacy_Address_Test,OU=Staff,DC=providence,DC=ketsds,DC=net)
4/15/2010 4:48:18 PM	496	OLPSRegistry	Info	User Updated (CN=User\, Test,OU=Legacy_Address_Test,OU=Staff,DC=providence,DC=ketsds,DC=net)
4/7/2010 5:56:32 PM	496	OLPSPowerShell	Info	Mailbox modify for 'Test.User@providence.kyschools.us' completed.
9/16/2009 4:16:04 PM	496	OLPSPowerShell	Info	Mailbox modify for 'Test.User@providence.kyschools.us' bypassed because of no changes.
9/10/2009 2:58:44 AM	496	OLPSRegistry	Info	User Updated (CN=User\, Test,OU=Legacy_Address_Test,OU=Staff,DC=providence,DC=ketsds,DC=net)
8/20/2009 1:30:26 PM	496	OLPSRegistry	Info	User Created (CN=User\, Test,OU=Legacy_Address_Test,OU=Staff,DC=providence,DC=ketsds,DC=net)

3.1.7.2 KETS Control Panel – End User Password Resets

Users have the ability to reset their Windows Live ID (Outlook Live) password separate from their Active Directory account password. This functionality is needed for times when the user has reset their Active Directory password and, for some reason, OLPS didn't sync the password change successfully to Outlook Live. If there were a network outage, for instance, that caused OLPS to miss a sync of a changed password, the end user could simply reset their Active Directory password again when the network is back up. Users should perform this step anytime they cannot login to OWA/Outlook but can login to Active Directory (or reset the AD password as explained above). The user MUST type their existing Active Directory password. This is done at https://mail.kyschools.us/password.aspx

3.1.8 Exchange Control Panel for Staff

The Exchange Control Panel (also known as the Outlook Live Control Panel) is a web interface that allows for common mailbox administration tasks in Outlook Live. Most everything an administrator in KETS would need to accomplish is done in Active Directory Users and Computers, thanks to the implementation of OLPS, except for Distribution Group management. The Exchange Control Panel will only need to be leveraged for Distribution Group or mailbox administration for the Staff GAL. To access, login to http://outlook.com, then selecting 'Options' at the upper right. Select My Organization from the dropdown as shown below.



There are more results available than are currently displayed. Enter a complete or partial display name in the search box above to f

Display Name	E-Mail Address
Allen, Johnny	John.Allen@Martin.kyschools.us
Arnold, Donald - DCPS	Donald.Arnold@daviess.kyschools.us
athletic.boosters	athletic.boosters@ludlow.kyschools.us
Ayers, Rose - EVES	rose.ayers@daviess.kyschools.us

For Staff, you can perform common tasks like change memberships of DGs, create mailboxes, etc. Understand that most tasks are automatically performed against objects in Active Directory as districts create and modify those objects, so there may be no need to utilize this function other than DG management.

If districts choose to create mailboxes or DGs with Exchange Control Panel it is important to understand that these objects will NOT pass through the OLPS system. There will not be an equivalent AD object created, nor will there be any records keeping for these objects. OLPS keeps track, for instance, all SMTP addresses that IT assigns. This verifies that there are no duplicates. If a mailbox object is created using Exchange Control Panel, it would set the SMTP address automatically within Outlook Live. If afterwards a user is created in Active Directory Users and Computers that had the same name (First Name and Last Name which concatenated together match the SMTP address of the mailbox) OLPS would get an error.

There are occasions where it makes sense to create mailboxes that do not have an associated AD object, or Distribution Groups that do not have a corresponding Security Group in AD. It's important to think through the requirements and results before administering.

3.1.9 Naming of Objects and GAL Visibility

As discussed in the section entitled *Outlook Live and GAL Visibility* there is one Staff Global Address List with no other Global Address Lists or Address Lists to segregate 'district only' users. This means that any user that requires e-mail access that is set as 'Staff' for *User Type* will show in the Staff GAL, which will show in the GAL for all staff in the state. It's imperative that districts utilize solid naming standards to segregate as much as possible their objects, specifically Distribution Groups. This is very important to convey to district staff as any user with a mailbox can create a Distribution Group which will be visible to all KETS Staff.

3.1.9.1 Naming of Distribution Groups

In the Outlook Live environment all staff Distribution Groups will be seen by all staff in the state, not just by the 'creating' district. Therefore proper naming of objects is critical. With that in mind it is in the district's best interest to apply verbose naming standards when creating any objects. All groups should begin with the district name followed by either a 'Co' or 'Ind' designation, then the purpose of the group.

District administrators, and end users, should use the following standard when naming Distribution Groups (or possibly other accounts, like Conference Room, Library, etc):

District *scope/purpose*

Examples:

Adair Co HS Teachers

Franklin Co Western Hills High School Library

Jackson Ind Coaches

To assist with this, KIDS will be placing the district name in the Company field of user objects which will help in distinguishing objects with similar/same names in the Global Address List. This does *not* however apply to Distribution Groups which do not have a Company attribute. The *Company* attribute in AD will not be populated by OLPS, only the Outlook Live account for GAL visibility.

End users now have the ability to create groups as discussed in section entitled *User-created Shared Distribution Groups*. With that stated staff end-users need to understand the importance of a solid naming standard for Distribution Groups as well as administrators.

3.1.9.2 Naming of Resource Accounts

Any resource account which must be visible in the GAL should be given a display name which begins with the name of the district. In this way, all of a given district's resource accounts will be clustered together in the GAL rather than dispersed throughout it. This is important since any GAL entries will be visible to the entire state rather than just a particular district.

Similar to Distribution Groups, district administrators should use the following standard when naming resource accounts.

District *scope/purpose*

Examples:

Scott Co Board Office Conference Room

Somerset Ind Community Questions

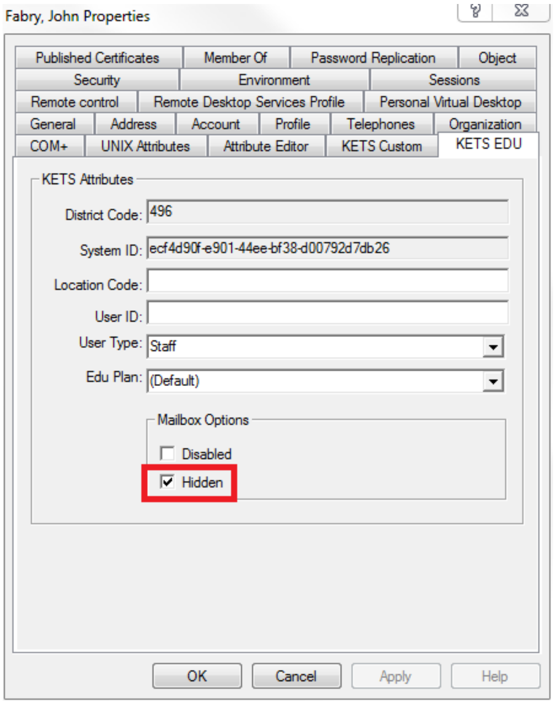
Woodford Co Help Desk

Note: Please be mindful of whether or not resource accounts actually need to be mail enabled. Resource accounts used purely for authentication purposes and which will never receive mail should not have a mailbox. Any such accounts should be set to NoMail on the KETSEDU tab in ADUC before provisioning to ensure it does not receive a mailbox, as per section 3.1.1 of this document.

Accounts which need to receive mail but which do not need to searchable in the GAL should be hidden. The steps to accomplish this are described in the next section, 3.1.9.3.

3.1.9.3 Distribution Group and Service Account GAL Visibility

Objects placed in any OU called '_Groups' will not be provisioned. Also, district administrators will continue to have the functionality to make Mail enabled objects "hidden" from the GAL. Hiding items from the GAL requires two steps. The first is to hide it from KDE by using the "Hidden" attribute on the KETS EDU tab in Active Directory Users And Computers (ADUC). See section 3.1.1 for instructions on installing the KETS EDU tab. Simply check the box and the account should be hidden from KDE users after the next run of provisioning:



KETS Attributes

District Code: 496

System ID: ecf4d90f-e901-44ee-bf38-d00792d7db26

Location Code:

User ID:

User Type: Staff

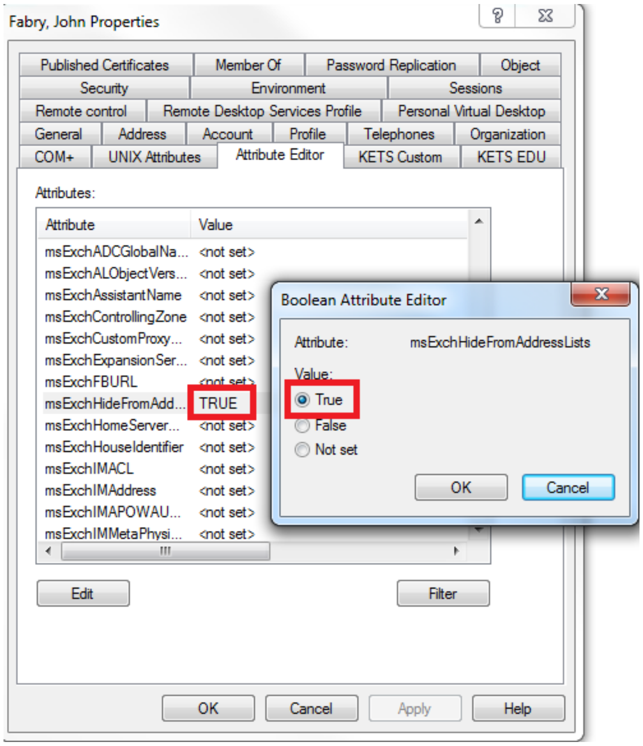
Edu Plan: (Default)

Mailbox Options

□ Disabled

☑ Hidden

The second step is to hide the account from the other state agencies with which KDE shares a GAL. This is done via the Attribute Editor tab in ADUC. To see this tab, you must enable Advanced Features in ADUC by going to **View > Advanced Features**. It is also important to note that the Attribute Editor tab is *not* visible if you are looking at an account via ADUC's Find feature. You must navigate to the appropriate OU and view the account's properties from there. Once the Attribute Editor tab is open, look for the **msExchangeHideFromAddressLists** attribute and ensure that it is set to TRUE.



Attributes:

Attribute	Value
msExchADCGlobalNa...	<not set>
msExchALObjectVers...	<not set>
msExchAssistantName	<not set>
msExchControllingZone	<not set>
msExchCustomProxy...	<not set>
msExchExpansionSer...	<not set>
msExchFBURL	<not set>
msExchHideFromAdd...	TRUE
msExchHomeServer...	<not set>
msExchHouseIdentifier	<not set>
msExchIMACL	<not set>
msExchIMAddress	<not set>
msExchIMAPOWAU...	<not set>
msExchIMMetaPhysi...	<not set>

Boolean Attribute Editor

Attribute: msExchHideFromAddressLists

Value:

● True
○ False
○ Not set

3.1.10 User Name Changes

When a user requires their user credential’s name changed it can be done within Active Directory by changing *First Name* and/or *Last Name*, by highlighting the user object in ADUC > click F2 to rename > change the name > you will then be presented a popup that will show other values you can choose to rename as well. It’s suggested to correct the name in all places presented and hit OK.

The corresponding SMTP Address, UPN Login and Windows Live ID will also be changed to reflect the new name. The previous SMTP Primary Address before the name change will become a Secondary Proxy Address, so the mailbox will continue to receive mail sent to the old SMTP Address.

3.1.11 E-mail Addresses and Secondary (Proxy) Addresses

The standard format for a Staff user’s SMTP address is :

FirstName.LastName@district.kyschools.us

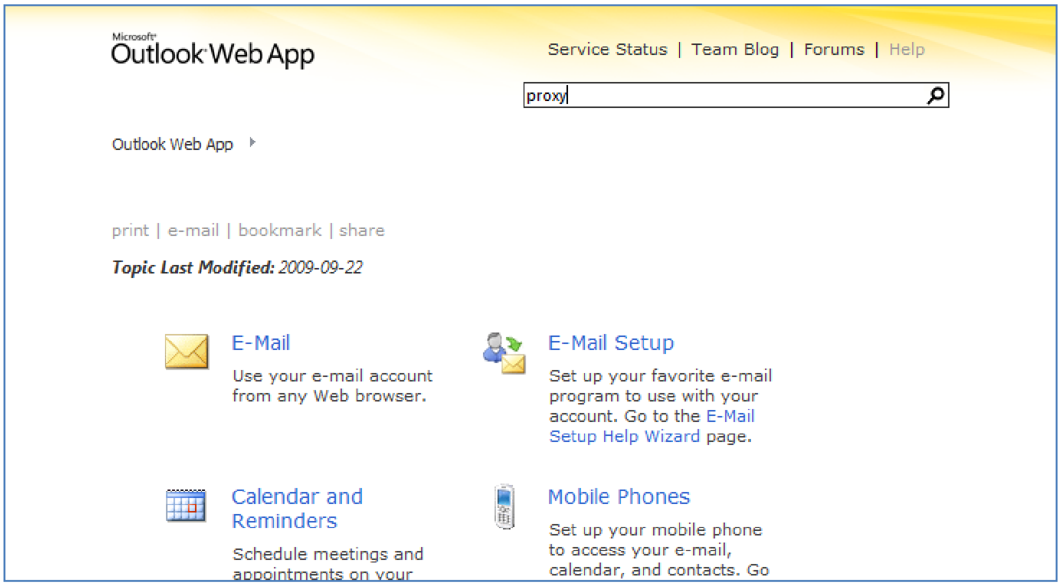
Districts can choose their own formatting for Students, whether adopting the above or starting the prefix with the graduation year, etc.

Note**: A period ‘.’ is the only non-alphanumeric character that should be in the SMTP address.** All other characters other than periods should be considered as invalid. This includes apostrophe ‘, double-quotes “, and ticks ` and slashes / \, etc

For Staff, districts have the ability through PowerShell to create secondary addresses to Outlook Live for staff (there is an example of the PowerShell cmdlets under the ‘PowerShell’ section later in this document). Alternately districts that require additional e-mail addresses such as ‘webmaster’, 'administrator', etc could create additional 'resource' user objects in ADUC with the appropriate naming. Districts could then choose to access these additional mailboxes with https://outlook.com or configure an Inbox Rule in the resource mailbox to flow messages to the desired mailbox (http://help.outlook.com/en-us/140/ms.exch.ecp.learnredirectto.aspx). The user could also from OWA choose to 'Open other user's' Inbox to access the 'resource' mailbox.

Note: You may notice that every Staff mailbox has a Secondary E-mail Address following the standard FirstName.LastName.district@staff.kyschools.us. This address was used during the migration from on-premise Exchange 2003 to Outlook Live. Please do not delete this address as it could become useful in the future.

For Students, through the Exchange Control Panel you can add Secondary addresses if desired. To find information on how to add additional SMTP addresses to student mailboxes go to http://help.outlook.com and search for 'proxy' as shown below.


Microsoft Outlook Web App

Service Status | Team Blog | Forums | Help

proxy

Outlook Web App

print | e-mail | bookmark | share

Topic Last Modified: *2009-09-22*

E-Mail

Use your e-mail account from any Web browser.

E-Mail Setup

Set up your favorite e-mail program to use with your account. Go to the E-Mail Setup Help Wizard page.

Calendar and Reminders

Schedule meetings and appointments on your

Mobile Phones

Set up your mobile phone to access your e-mail, calendar, and contacts. Go

3.1.12 Notification of OLPS errors

As discussed OLPS is responsible for the management of mail enabled objects between Active Directory and Outlook Live. OLPS runs jobs at different intervals. These by default are once every 15 minutes for Staff (could take up to an hour with replication latencies), every 6 hours for Students and once at night for groups/contacts (there are not groups or contacts that flow to the Student Tenant). In the event that there are errors on a run of provisioning the information about the specific failure(s) is sent to any member of the DG called notifications@district.kyschools.us, where district is the district's SMTP Domain Name. This group should be populated with the desired member(s), utilizing the OutlookAdmin account, in the Exchange Control Panel. Notice that OutlookAdmin is set as owner instead of DLAdmin.

3.2 Password Complexity Requirements

It always makes good security sense to implement aggressive password policies. In Live@edu it's required to have a six character password. Districts must either inform users requiring a mailbox to specify at least a six character password, or set policies within Active Directory which force at least this minimum requirement. Forcing a policy requirement can be accomplished with the Default Domain Security Policy (requires a KETS Service Desk request) which affects all users in the domain, or by implementing Fine-Grained Password Policies (discussed in detail in the following section).

The following rules and restrictions apply to passwords for Outlook Live accounts. This means that **these requirements must also be met on the Active Directory user account passwords that require mailboxes.**

Rules

- The minimum length is six characters.
- The maximum length is 16 characters.
- Strong passwords are at least eight characters long.
- The password is case-sensitive.
- The password can contain uppercase and lowercase letters, and numbers.
- The password can contain the following ASCII text characters: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /

Restrictions

The password can't contain:

- Spaces
- Non-English characters
- The alias part of the e-mail address. For example, if the e-mail address is user@contoso.edu, the password can't contain user. This restriction isn't case-sensitive, so USER or User can't be used in the password for user@contoso.edu.
- The answer to the Windows Live ID secret question that helps users reset their password. For example, if the Windows Live ID secret question is Mother's birthplace, and Seattle is the answer, the password can't contain Seattle. This restriction isn't case-sensitive, so SEATTLE or seattle can't be used in the password.

Note: Due to the engineering behind the solution, it is technically possible for a user with a mailbox to NOT have a six character password limit. For users who only accesses email through the KETS OWA link (https://mail.kyschools.us) from inside the school district on a computer that is joined or bound to the domain, the user will be authenticated with SSO (Single Sign-On). With SSO through OWA, and technologies implemented for KETS, mail enabled users do not have to have a six character password. Districts must realize, though, other access mediums to mail will not allow the user to authenticate without a six character password, namely: Active Sync devices, Mail Access from a Mobile Phone, *Authentication from an Outlook 2007 MAPI Client and OWA through Outlook.com.*

3.3 Fine-Grained Password Policies

In Windows Server 2003 Active Directory a domain is a password policy boundary meaning that a single password policy applies to all users in an Active Directory domain. There is a new technology in Windows Server 2008 Domain Service (Active Directory) called Fine-Grained Password Policies which enables the use of granular password policies for subsets of users within a domain. This new technology is an extension of the existing Default Domain Password Policy (explained later). Districts have the ability to utilize any of six new policies for different groups of users. This is essential as it will be a requirement with the new messaging system, Outlook Live, which requires the use of Windows Live IDs. A Windows Live ID requires a six character password (there are no other requirements beyond that to change passwords or complexity settings, etc).

A district can choose to utilize only the default domain policy but will have the ability to take certain groups of users, students for example, and apply different password policies from the staff. The Default Domain Password Policy affects all users in a domain that are not members of one of the Fine-Grained Password Policy Groups. These new policies are not implemented on an OU basis. They are assigned to security groups and/or users (discussed below).

Fine-Grained Password Policies work with the Default Domain Password Policy through 'precedence' or weighting. The Default Domain Password Policy has the lowest weight, meaning if a user is placed in any of the password policy groups (explained below) the group policy will be applied instead of the Default Domain Password Policy. The groups have weighting as well, so users can be in multiple groups but only the group policy with the highest weighting will be applied to that user.

If a district chooses to utilize the Default Domain Password Policy they must ensure that it meets the minimum requirements for mailbox access. If a district would like to utilize the default policy and needs to modify it they need to contact the KETS Service Desk. It must be reiterated that ANY user who requires a mailbox MUST have at least a six character password. Because of this one of the password policies will match that minimum (six characters, never change password and no complexity).

Six Global Security Groups exist which reside in the *_District Admins, Users and Groups OU.* Each of these groups maps to a corresponding Fine-Grained Password Policy. For a given policy to be applied users must be placed in that corresponding group. The groups and explanation of each follow.

DIST Password Policy - None

This policy requires no minimum password length, no complexity, forces no change and has a zero password history.

DIST Password Policy - Three Never

This policy requires a three character password length minimum, no complexity, forces no change and has three passwords remembered (meaning you cannot reuse the last three passwords)

DIST Password Policy - Six Never

This password policy matches the minimum requirements to received mailbox access. This policy requires a six character password length minimum, no complexity, forces no change and has a zero password history

DIST Password Policy - Six Complex 60

This policy requires a six character password length minimum, forces complexity*****, forces a change at 60 days and has five passwords remembered (meaning you cannot reuse the last five passwords)

DIST Password Policy - Eight 60

This policy requires an eight character password length minimum, no complexity, forces a change at 60 days and has three passwords remembered (meaning you cannot reuse the last three passwords)

DIST Password Policy - Eight Complex 30

This policy requires an eight character password length minimum, forces complexity*, forces a change at 30 days and has twelve passwords remembered (meaning you cannot reuse the last twelve passwords)

* For those policies above which require complexity the user must meet at least three of the following four complexity rules within the password:

- Uppercase characters (A through Z)
- Lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Special symbols or non-alphabetic characters (for example: !, $, #, %, etc.)

The precedence of these groups goes from the lowest precedence "**DIST Password Policy – None"** to the highest precedence "**DIST Password Policy - Eight Complex 30"**. This is with the understanding that the Default Domain Password Policy ultimately has the lowest precedence. To that end if a user is a member of any of these groups the group policy is applied instead of the Default Domain Password Policy. Also, if there are settings defined on the actual user object ('Password Never Expired', etc) those settings will apply no matter what policy the user is associated with.

Example: If a user is in both the '**DIST Password Policy - Three Never'** group and the '**DIST Password Policy - Eight 60'** group the user would have to meet the requirements of the DIST Password Policy – Eight 60 group.

When a user is placed in a Fine-Grained Password Policy group, or if the Default Domain Password Policy is modified, the affected users will NOT be required to immediately change their password to match the minimum requirements. The next time the user will have to change their password the new policy would be applied at that time. If a user currently has no password policy that requires them to change their password the user would either have to be instructed to change their password manually or the user object would need to be set to 'User must change password at next logon'. This can be accomplished either in Active Directory Users and Computers on a per user basis or through a script (VB, LDIFDE, etc) which would modify the pwdLastSet attribute to 0 (zero) on each user object. District will also have the ability to change the password on behalf of the user through whatever means they may do this today, as long as the password is reset/changed the system will synchronize the Active Directory password to Outlook Live.

Note: There appears to be a 'bug' with Fine-Grained Password Policies in that the message that some clients will receive when changing their password can be different than what should be presented. Some versions of Windows tested (Windows 7, Vista) provided a generic message when a user password change was attempted that didn't meet the minimum requirements of the Fine-Grained Password Policy:

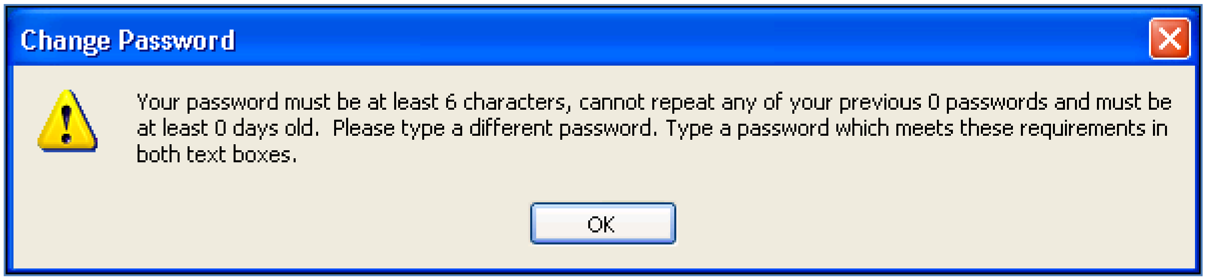
Unable to update the password. The value provided for the new password does not meet the length, complexity, or history requirement of the domain.

This isn't very helpful, but it's acceptible in that it doesn't provide inaccurate information. Also it is good for security reasons as it doesn't show a person trying to guess another users password any minimum requirements. It's important to note that all versions/service packs were not tested, only Windows 7 RC and Vista Ultimate SP2. Other versions may react differently, possibly as described below. It's also important to note that the Fine-Grained Password Policies all worked well functionally in testing, the only issue as explained here it the message that results from a user trying to change their password to something that doesn't meet the resultant policy for that user.

With Windows XP SP3 testing results were different. Testing results:

If a user has a Fine-Grained Password Policy assigned and tries to change their password to a password that doesn't meet the minimum requirements of the FGPP that user will receive a popup (which is expected), but the information in the popup applies to the Default Domain Policy settings, not the Fine-Grained Password Policy settings that the user actually is held to.

Example: The Default Domain Password Policy for your district is 6 character, 0 history and 0 min days. You assign a user to the 'DIST Password Policy – Three Never' group. This policy is the same as the default domain policy, other than the password length must be at least 3 characters instead of 6 in length. If the users tries to change their password to a password that is 2 characters in length they will receive the following message:



Your password must be at least 6 characters, cannot repeat any of your previous 0 passwords and must be at least 0 days old. Please type a different password. Type a password which meets these requirements in both text boxes.

This is incorrect, as the user in the example would only need to supply a password of 3 characters as a minimum. This is the same if the user was placed in the 'DIST Password Policy – Eight Complex 30' group, which requires a password of at least 8 characters, complexity enabled and a 30 day maximum age. If a person in this group tried to change their password to something that didn't meet the requirements, say only 7 characters, it would still present the above image which again is incorrect and will cause confusion.

KIDS has worked with Microsoft on this ‘issue’. It has been decided that since this is a client message which has been ‘resolved’ on newer clients with a generic message there will not be a ‘fix’. If districts wish to utilize Fine-Grained Password Policies this will be confusing for some users so please educate them on this item.

3.4 SPAM Protection for Staff and Students

It’s important to note that in this initial iteration of Outlook Live there is not a SPAM solution built which is comparable to Exchange Hosted Services. We have, however, built some customized settings to give us as much flexibility as possible. The future plan is to have Forefront Online Protection for Exchange – FOPE – embedded in the product with Office 365. But for the current time let’s discuss the current environment.

For Students, logged in as **OutlookAdmin@stu.district.kyschools.us** , you can modify many filtering type settings in the Exchange Control Panel (which are discussed in detail in Section 3. For Staff, however, this flexibility is not available. We have implemented some basic functionality for Staff that, while not as rich as an EHS offering, hopefully will allow us to have an adequate system until the Office 365 migration. Until then it should be noted that the only ‘whitelisted’ addresses for Outlook Live for Staff are those SMTP IP Addresses for kyschools.us and ky.gov (as well as LRC.ky.gov). The system does not allow for domain names to be entered, only IPs. Those IPs should be ‘owned’ by the entity requesting so until we have the EHS/FOPE functionality please be advised that there is a chance that valid mail could get filtered as it is not bypassing the filter rules.

Out of the box, Outlook Live sets SPAM Confidence Levels (SCLs) to each e-mail (just as EHS does). The higher the SCL the more probable the message is SPAM. We have modified the Transport Rules for **Students only** so that certain levels get ‘Quarantined’. Quarantining is not a default option with Outlook Live. With that stated, a mailbox has been created for each Student tenant (ex. quarantine@stu.barren.kyschools.us) who will receive any messages with SCL equal to 5 or 6. SCLs of 7 and above are deleted, while SCL 4s are delivered to the ‘Junk Mail’ folder in the client. SCLs of 1-3 are delivered to the Inbox of the students.

3.4.1 ‘Quarantine’ mailbox

As stated in the above section each district has a mailbox for students (Quarantine@stu.*district*.kyschools.us). This is a normal user mailbox like any other. The difference is that there is a Transport Rule set for all messages sent to students which evaluates the SCL levels on incoming messages. If the SCL level is either 5 or 6 (meaning it is potential SPAM) it will move these messages to the ‘Junk Mail’ folder of the appropriate Quarantine mailbox instead of the Student’s mailbox. **Check this mailbox often** for valid (false-positive) e-mails, and purge any unwanted junk mail. Unlike other systems (like EHS) there is no ‘Release’ type option. Districts should log in to this mailbox using www.outlook.com, not mail.kyschools.us. The process would be:

- Identify False-Positives (mail that should not have been quarantined
- While the message is closed, Right-click the message and select ‘Forward as attachment’, forwarding to the original recipients

3.4.2 Attachment Allow/Block lists through Outlook Live

The following link shows the attachment extensions which are allowed through the Live@edu system. Note that the web page discusses changes that can be made in Exchange 2010 by administrators as well as other settings. This is to be ignored. The only pertinent information for this discussion is the table in the web link which shows the different file types that are allowed or blocked. This link is being provided as the content within the table could change over time, and would not be valuable if copy/pasted statically into this document.

http://technet.microsoft.com/en-us/library/bb124232(EXCHG.140).aspx

3.4.3 Reporting SPAM to Microsoft

In the event that users are receiving SPAM emails, a report can be filed with Microsoft which will help in deterring those types of messages. Two options are available:

1. Users that access email using the Outlook client can use the Outlook Junk Mail Reporting Add-in. This add-in, users have a one-click interface for submitting SPAM to the FOPE SPAM Team for analysis.
    - This tool can be downloaded by navigating to Microsoft.com and searching for "Outlook Junk Mail Reporting Add-in".
    - Download and install the appropriate Add-in for the version of Outlook being used
2. Users that access email using a method other than the Outlook client can submit messages to Microsoft by creating a new email and attaching the SPAM messages to it. They can send this email to abuse@messaging.microsoft.com for analysis. It is important to attach the SPAM messages to a new email rather than just forwarding it so that the full headers can be examined.

3.5 Exchange Control Panel for Students

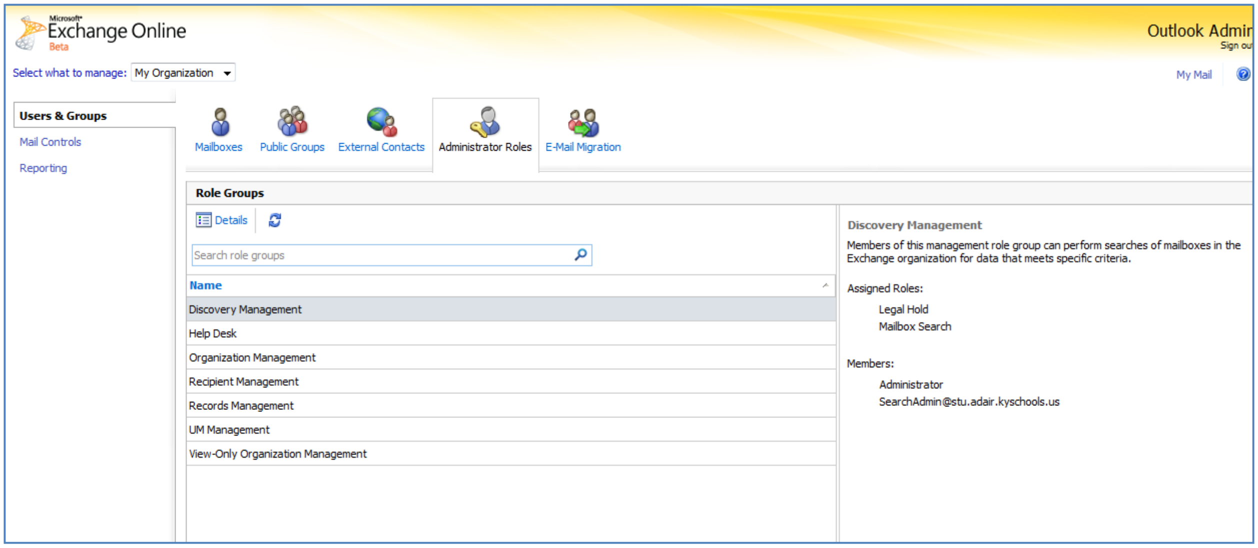
The following information applies to management of the Student Tenant (GAL) only. The focus is on administering the backend configuration settings, not user administration. Most of these tasks are specific for the Student environment, not the Staff. As the Staff Tenant encompasses all staff in the state its configuration and access is reserved by KIDS on behalf of the districts.

Districts can perform Tenant settings (discussed below) by logging into http://outlook.com as OutlookAdmin@stu.district.kyschools.us, then choosing 'Options' from the top right.

There are several student-specific settings that can be applied which affect the student e-mail experience. There are three areas you can choose on the left pane; *Users and Groups, Mail Controls* and *Reporting*. Under '*Users and Groups*' you can perform normal mail administration (create mailboxes, DGs, etc). Administrator Roles is a way to give 'privileged access' to certain user groups if desired. This is discussed below.

3.5.1 Role-Based Access Control (RBAC) for Students

RBAC Roles are pre-configured roles which can be assigned to different users for granular administration within Outlook Live for students. This can be accomplished for the built-in roles through Exchange Control Panel. An administrator can also create custom roles, for instance, that only has password reset permissions in Outlook Live (not in AD). Before you begin working with RBAC roles you should have a solid understanding of what Management Roles in Outlook Live.



Role Groups

Name
Discovery Management
Help Desk
Organization Management
Recipient Management
Records Management
UM Management
View-Only Organization Management

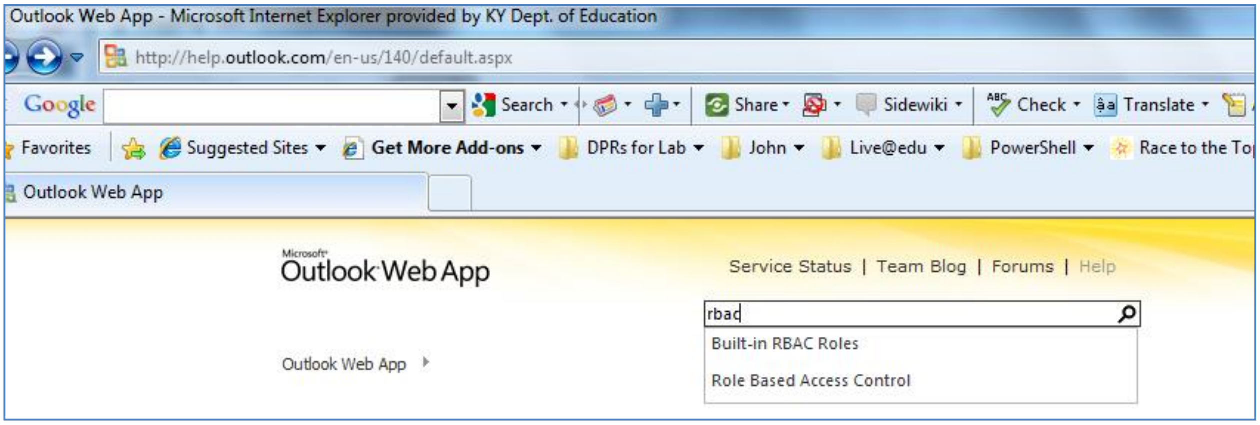
Discovery Management

Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.

Assigned Roles:
Legal Hold
Mailbox Search

Members:
Administrator
SearchAdmin@stu.adair.kyschools.us

You can always search help.outlook.com for RBAC for more information.

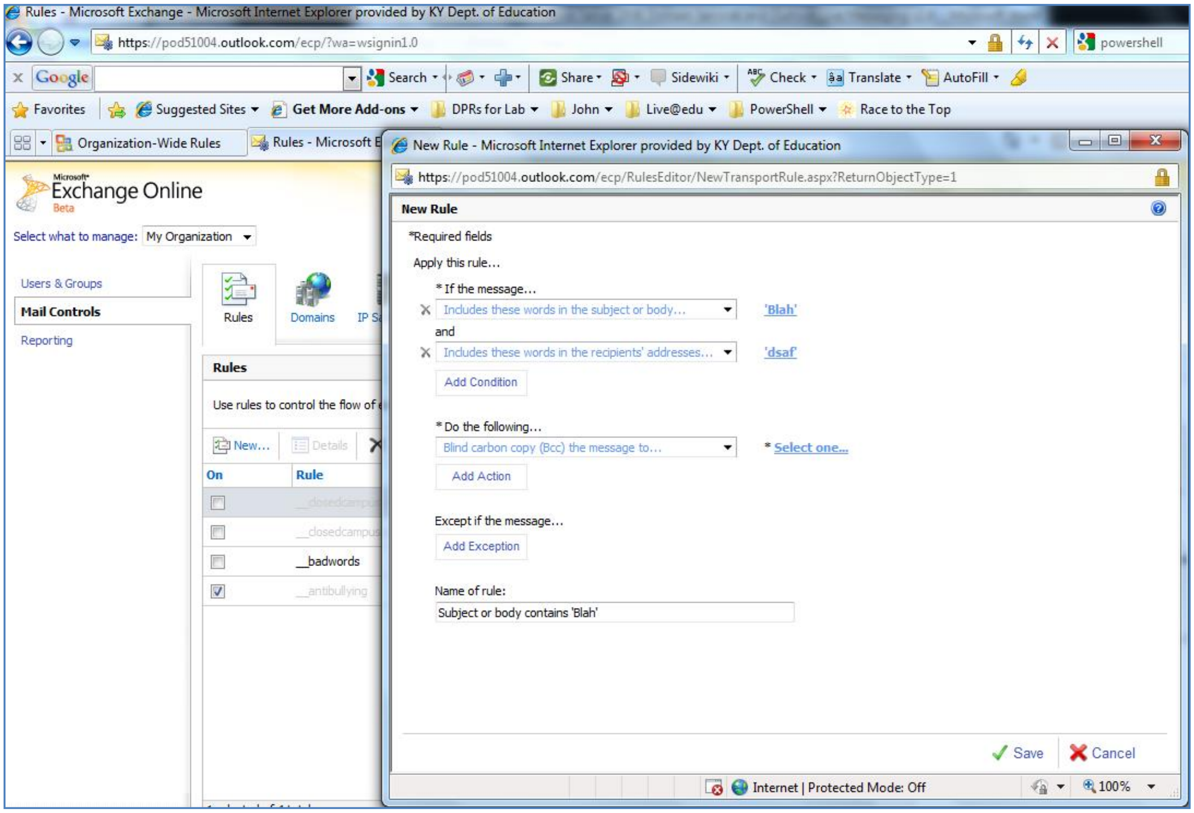

Outlook Web App - Microsoft Internet Explorer provided by KY Dept. of Education
http://help.outlook.com/en-us/140/default.aspx
Google
Search
Share
Sidewiki
Check
Translate
Favorites
Suggested Sites
Get More Add-ons
DPRs for Lab
John
Live@edu
PowerShell
Race to the To
Outlook Web App
Microsoft Outlook Web App
Service Status | Team Blog | Forums | Help
Outlook Web App

rbac
Built-in RBAC Roles
Role Based Access Control

3.5.2 Transport Rules for Students

Transport Rules, or simply ‘Rules’, within Outlook Live are a very powerful way to control mail-flow to and from students in your district. These rules can affect all Student mailboxes for a district, or can be scoped to only affect mail between two users (or one for that matter). You can choose to add conditions so that the logic can become Boolean. Once the condition is met you can choose between several end results (do not send the message, BCC someone, etc).

***Note:** Transport Rules can also be configured using PowerShell. Using PowerShell will open up extremely granular controls in the creation and configuration of Transport Rules for Students, enabling districts to allow/block based on many, many different scenarios. Refer to the section in this document on '**PowerShell – Examples – Transport Rules'** for more information.*



Rules - Microsoft Exchange - Microsoft Internet Explorer provided by KY Dept. of Education
https://pod51004.outlook.com/ecp/?wa=wsignin1.0
powershell
Google
Search
Share
Sidewiki
Check
Translate
AutoFill
Favorites
Suggested Sites
Get More Add-ons
DPRs for Lab
John
Live@edu
PowerShell
Race to the Top
Organization-Wide Rules
Rules - Microsoft E
Microsoft Exchange Online Beta
Select what to manage: My Organization
Users & Groups
Mail Controls
Reporting
Rules
Domains
IP S
Rules
Use rules to control the flow of
New...
Details
On
Rule
__closedcampus
__closedcampus
__badwords
__antibullying
New Rule - Microsoft Internet Explorer provided by KY Dept. of Education
https://pod51004.outlook.com/ecp/RulesEditor/NewTransportRule.aspx?ReturnObjectType=1
Internet | Protected Mode: Off
100%

New Rule

*Required fields

Apply this rule...

* If the message...

✕ Includes these words in the subject or body... 'Blah'

and

✕ Includes these words in the recipients' addresses... 'dsaf'

Add Condition

* Do the following...

Blind carbon copy (Bcc) the message to... * Select one...

Add Action

Except if the message...

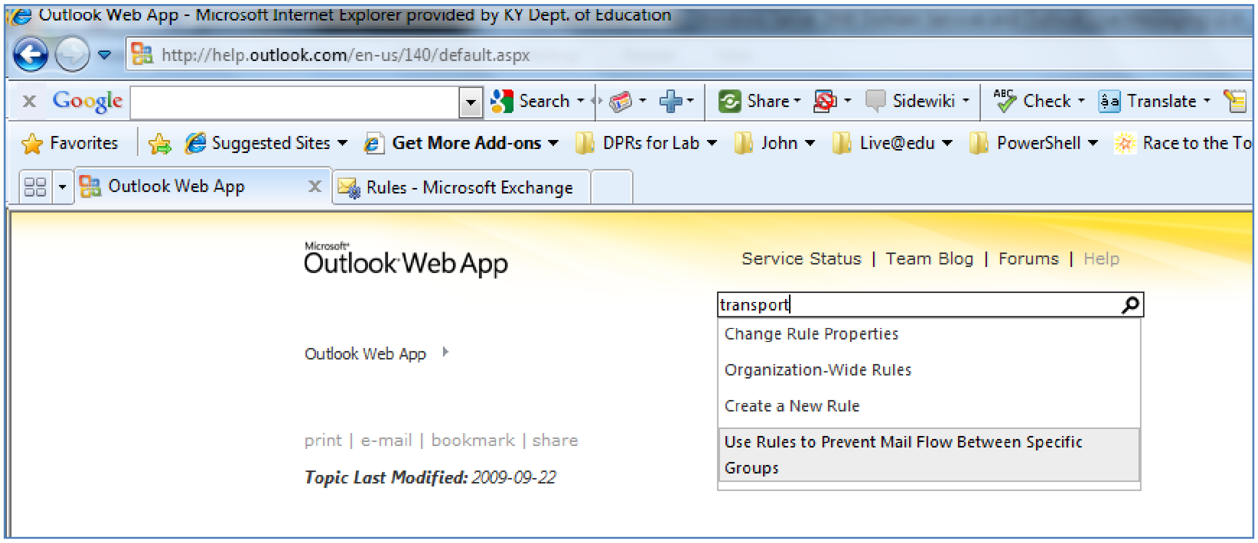
Add Exception

Name of rule:

Subject or body contains 'Blah'

✓ Save ✕ Cancel

For more information on Transport Rules search http://help.outlook.com



Outlook Web App - Microsoft Internet Explorer provided by KY Dept. of Education
http://help.outlook.com/en-us/140/default.aspx
Google
Search
Share
Sidewiki
Check
Translate
Favorites
Suggested Sites
Get More Add-ons
DPRs for Lab
John
Live@edu
PowerShell
Race to the To
Outlook Web App
Rules - Microsoft Exchange
Microsoft Outlook Web App
Service Status | Team Blog | Forums | Help
Outlook Web App
print | e-mail | bookmark | share

transport

Change Rule Properties

Organization-Wide Rules

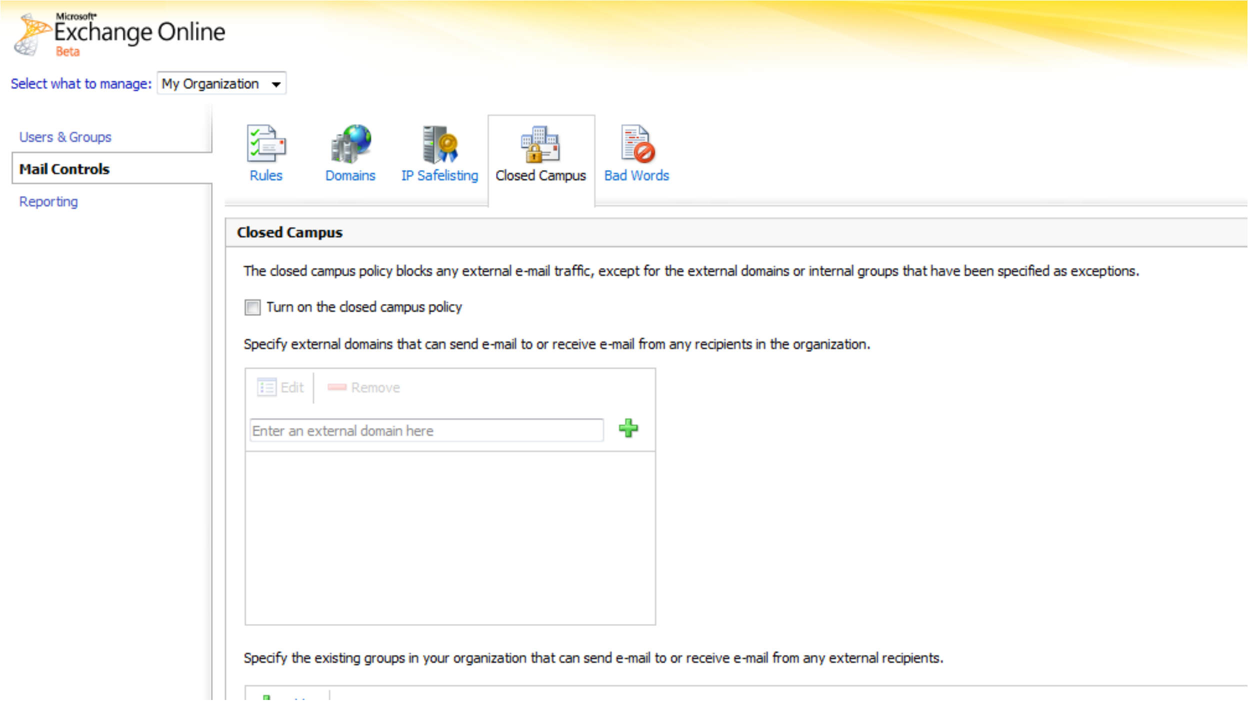
Create a New Rule

Use Rules to Prevent Mail Flow Between Specific Groups

Topic Last Modified: 2009-09-22

3.5.3 Closed Campus

By choosing the ‘Mail Controls’ option on the left you have several categories that can be set for students. One of these is the ability to set your Student Tenant to not receive e-mails from any domain other than those specified (like from your staff for instance). E-mail addresses that are allowed to send can also be set at a mailbox level if desired



Closed Campus

The closed campus policy blocks any external e-mail traffic, except for the external domains or internal groups that have been specified as exceptions.

□ Turn on the closed campus policy

Specify external domains that can send e-mail to or receive e-mail from any recipients in the organization.

Specify the existing groups in your organization that can send e-mail to or receive e-mail from any external recipients.

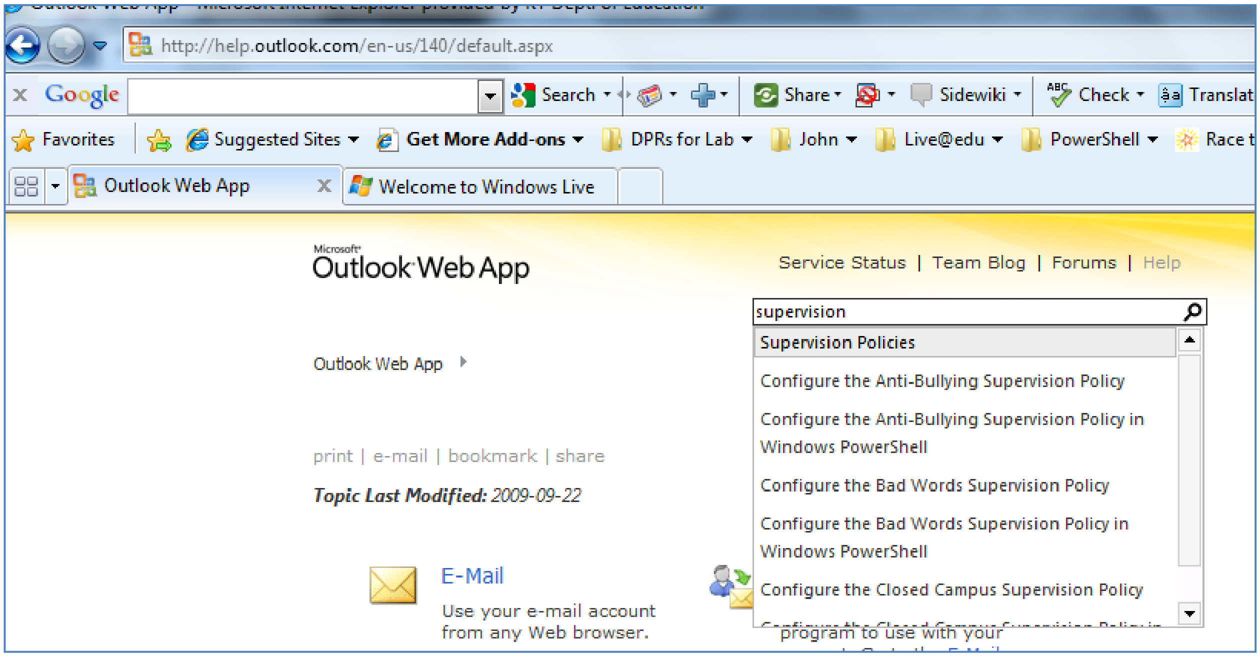
3.5.4 Safelisting (aka ‘Whitelisting’) for Students

Safelisting is the ability to place certain SMTP domains in a list which will allow those users from that domain to send e-mails to your students, bypassing any SPAM type filters, etc. This can restrict false-positive message blocking from those domains. In order for district administrators to create a “white list” of safe IP Addresses (Actions formerly performed in the EHS Admin interface) a ticket would have to be submitted to the KETS Service Desk.

Note: ‘Whitelisting’ for Staff is a statewide setting which is administered by KIDS on behalf of the districts. This means that any domain which is requested to be whitelisted for a given district would need to go through the KETS Service Desk, and would be whitelisted for all faculty and staff in all districts.

3.5.5 Supervision Policies (Anti-Bullying and Bad Words) for Students

There are special policies built within Outlook Live which are customized for K-12 entities. These policies are configurable through Remote PowerShell. To view information about these policies you can go to http://help.outlook.com and search for ‘Supervision’ as you see below, which will show the different configurable policies.



Topic Last Modified: 2009-09-22

supervision

Supervision Policies

Configure the Anti-Bullying Supervision Policy

Configure the Anti-Bullying Supervision Policy in Windows PowerShell

Configure the Bad Words Supervision Policy

Configure the Bad Words Supervision Policy in Windows PowerShell

Configure the Closed Campus Supervision Policy

Two of the policies which districts may be of interest to districts are:

- **Anti-Bullying -** prevents e-mail communication between specific senders and individual users in your Outlook Live organization. The anti-bullying supervision policy helps you protect students from harassment e-mails. E-mail that is sent to the users you specify is rejected, and a non-delivery report (NDR) is generated.

- **Bad Words -** establishes "bad word" filters in your Outlook Live organization. A *bad word filter* searches messages for the specified words and prevents the delivery of messages that contain those words.

The Bad Words policy is configurable from within the Exchange Control Panel by the OutlookAdmin@stu.*district*.kyschools.us **Each district should go to this area and apply any bad words to restrict message flow to their students.** A screen shot can be seen in the section entitled *Exchange Control Panel.*

Note: Districts have the ability to create their own Rules in this interface, similar to Outlook Inbox Rules, to restrict or modify the mail flow of messages between users. These are actually ‘Transport Rule’ so PowerShell can be used as well for more granularity. Refer to the section in this document for creating Transport Rules using PowerShell for more info.

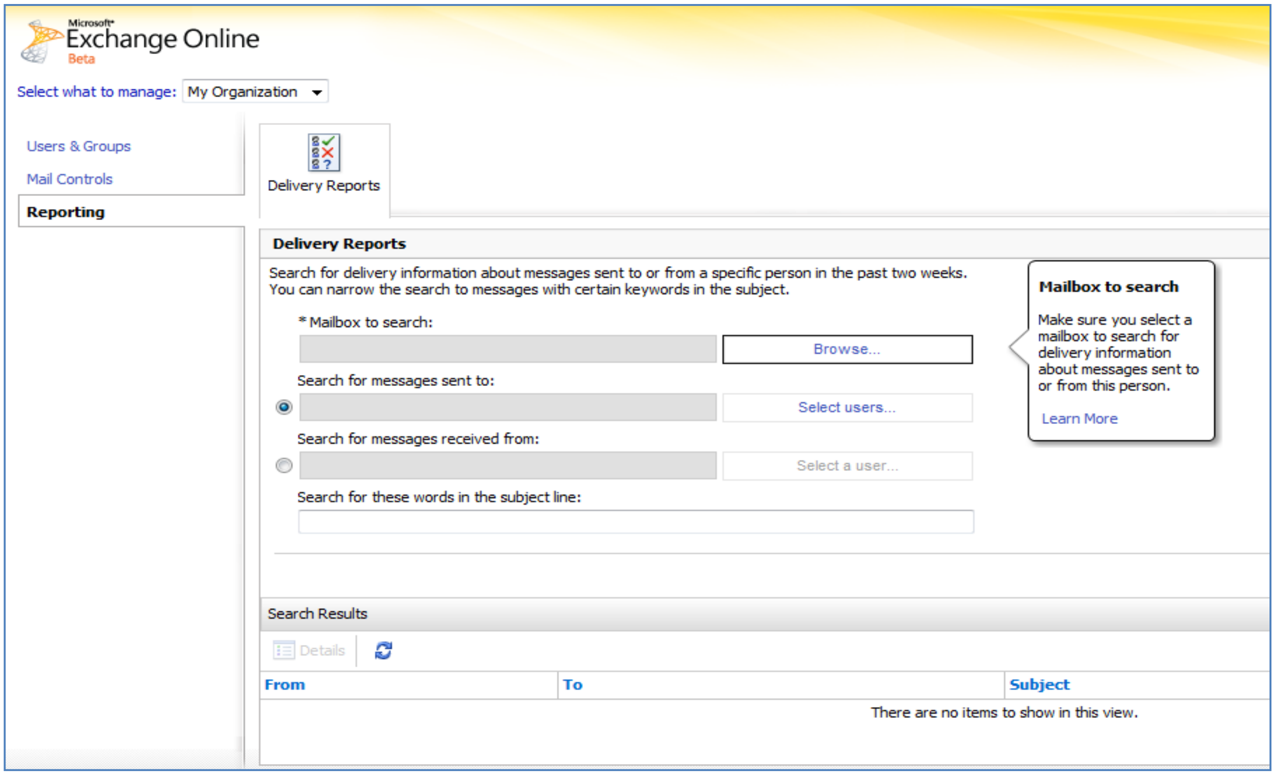
3.5.6 Student Object Administration

In addition to DG management (discussed in the previous section) administrators can also modify other objects within the respective district's Student Tenant (GAL). Remote PowerShell 2.0 can be used against Outlook Live (*for more information go to help.outlook.com and search for "Use Windows PowerShell"*) for object manipulation. District administrators must authenticate to the Student Tenant with the account OutlookAdmin@stu.district.kyschools.us (ex. OutlookAdmin@stu.woodford.kyschools.us). This account has full access in the corresponding Student Tenant.

Note: Any objects created/modified with PowerShell against the Student Tenant do not pass through the OLPS system.

3.5.7 Reporting for Students

OutlookAdmin can do searches for messages sent to/from specific users using the *Reporting* option. You can search back for messages sent within the previous 2 weeks. This permission can be assigned to other individuals. Leverage http://help.outlook.com for instructions.


Microsoft Exchange Online
Beta
Select what to manage: My Organization
Users & Groups
Mail Controls
Reporting
Delivery Reports

Delivery Reports

Search for delivery information about messages sent to or from a specific person in the past two weeks. You can narrow the search to messages with certain keywords in the subject.

* Mailbox to search:
Browse...
Search for messages sent to:
● Select users...
Search for messages received from:
○ Select a user...
Search for these words in the subject line:

Mailbox to search

Make sure you select a mailbox to search for delivery information about messages sent to or from this person.

Learn More
Search Results
Details

From	To	Subject

There are no items to show in this view.

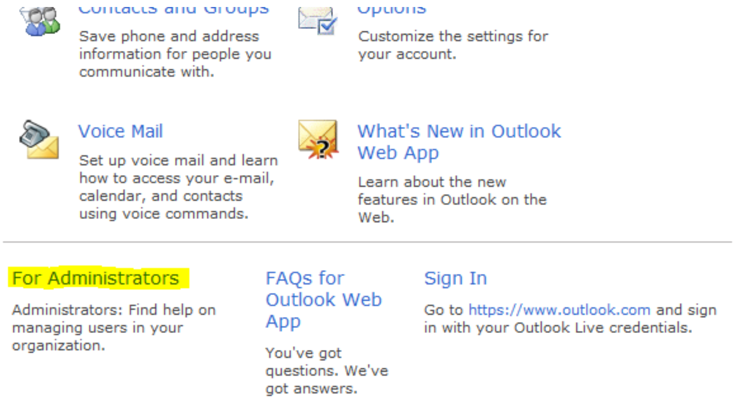
3.6 Windows PowerShell

Windows PowerShell is a task-based command-line shell and scripting language designed especially for system administration. Built on the .NET Framework, Windows PowerShell helps IT professionals and power users control and automate certain administrative tasks. The vast majority of all management tasks can be performed with either AD specific tools, the Exchange Control Panel or KETS Control Panel. There might be, however, certain tasks that districts may want to do, possibly in 'bulk', that can be performed with PowerShell. Some tasks can ONLY be performed with PowerShell.

For the Student Tenant districts can do extensive management tasks with PowerShell logged in as OutlookAdmin@stu.*district*.kyschools.us. For the Staff Tenant districts can do normal user/DG management logged in as OutlookAdmin@*district*.kyschools.us. Certain tasks, such as multi-mailbox searches (logged in as SearchAdmin@*district*.kyschools.us) can only be performed with PowerShell.

Windows PowerShell executable(s) are referred to as Windows Management Framework. This package contains Windows PowerShell 2.0, WinRM (for remote administration which is need to connect to Outlook Live), and ISE with is a graphical host which can be used to create or modify PowerShell scripts. Notepad or any text editor may also be used.

You can get started by going to help.outlook.com and choose 'For Administrators' at the bottom



Contacts and Groups

Save phone and address information for people you communicate with.

Options

Customize the settings for your account.

Voice Mail

Set up voice mail and learn how to access your e-mail, calendar, and contacts using voice commands.

What's New in Outlook Web App

Learn about the new features in Outlook on the Web.

For Administrators

Administrators: Find help on managing users in your organization.

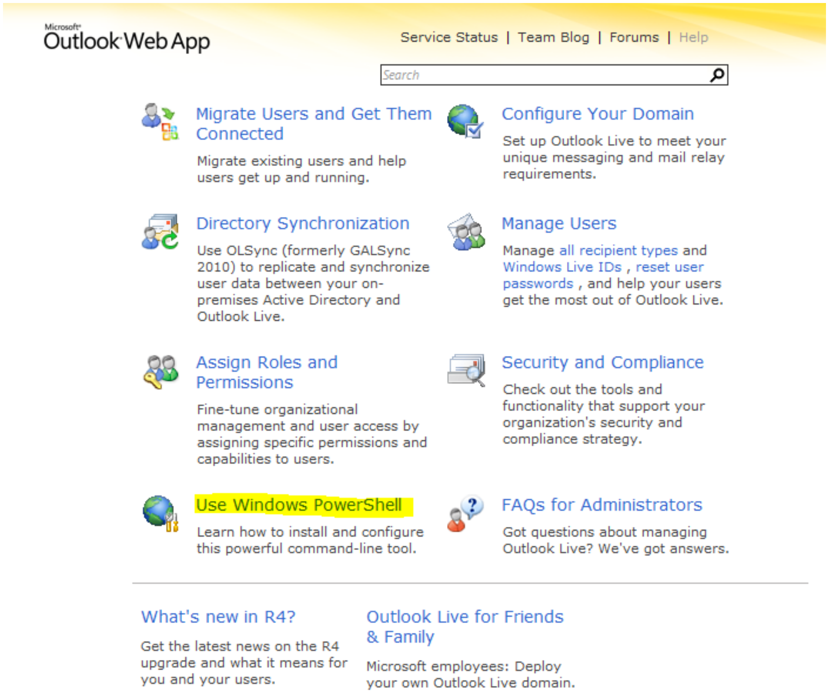
FAQs for Outlook Web App

You've got questions. We've got answers.

Sign In

Go to https://www.outlook.com and sign in with your Outlook Live credentials.

Next choose 'Use Windows PowerShell' from the presented options


Microsoft Outlook Web App
Service Status | Team Blog | Forums | Help
Search

Migrate Users and Get Them Connected

Migrate existing users and help users get up and running.

Configure Your Domain

Set up Outlook Live to meet your unique messaging and mail relay requirements.

Directory Synchronization

Use OLSync (formerly GALSync 2010) to replicate and synchronize user data between your on-premises Active Directory and Outlook Live.

Manage Users

Manage all recipient types and Windows Live IDs , reset user passwords , and help your users get the most out of Outlook Live.

Assign Roles and Permissions

Fine-tune organizational management and user access by assigning specific permissions and capabilities to users.

Security and Compliance

Check out the tools and functionality that support your organization's security and compliance strategy.

Use Windows PowerShell

Learn how to install and configure this powerful command-line tool.

FAQs for Administrators

Got questions about managing Outlook Live? We've got answers.

What's new in R4?

Get the latest news on the R4 upgrade and what it means for you and your users.

Outlook Live for Friends & Family

Microsoft employees: Deploy your own Outlook Live domain.

You will find information on how to install, connect and run PowerShell cmdlets and tasks from these instructional sources. It is important to note, however, that as discussed above there are some tasks that cannot be performed with PowerShell against the Staff Tenant.

In addition to the following examples there are accompanying videos for some common PowerShell tasks that can be viewed from the KETS Control Panel - https://live.kyschools.us/Admin/videos.aspx

3.6.1 PowerShell – Connecting to Outlook Live

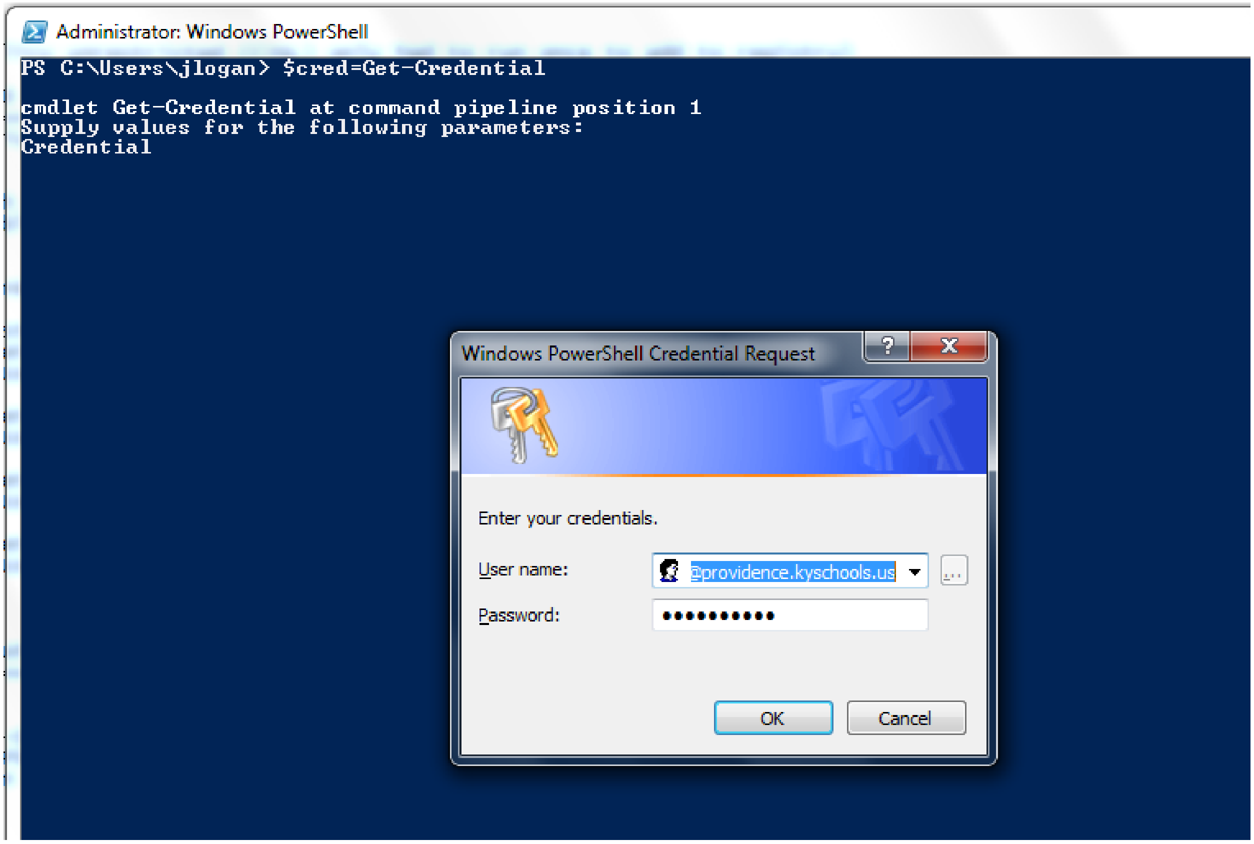
After installing the Windows Management Framework you can open the shell and begin. You must first start by connecting to Outlook Live for your domain. You must **proceed with caution** as there can be irreversible effects from running cmdlets without complete understanding of what you're doing.

Note: Depending on the PowerShell cmdlets you choose to run you may have to run the command 'set-executionpolicy unrestricted'. This is only run once (added to the registry) and allows non-trusted published scripts to run. Obviously run with caution.

To Connect to Outlook Live

```
$LiveCred = Get-Credential
```

Authenticate in the Forms windows that appears. Login as either OultookAdmin@... Or OutlookAdmin@stu... depending on which group of users you want to apply the setting to. Note that some of the cmdlets can only be used against the Student Tenant, which should be defined in the following sections.



Administrator: Windows PowerShell

```
PS C:\Users\jlogan> $cred=Get-Credential

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
```

Windows PowerShell Credential Request

Enter your credentials.

User name: @providence.kyschools.us

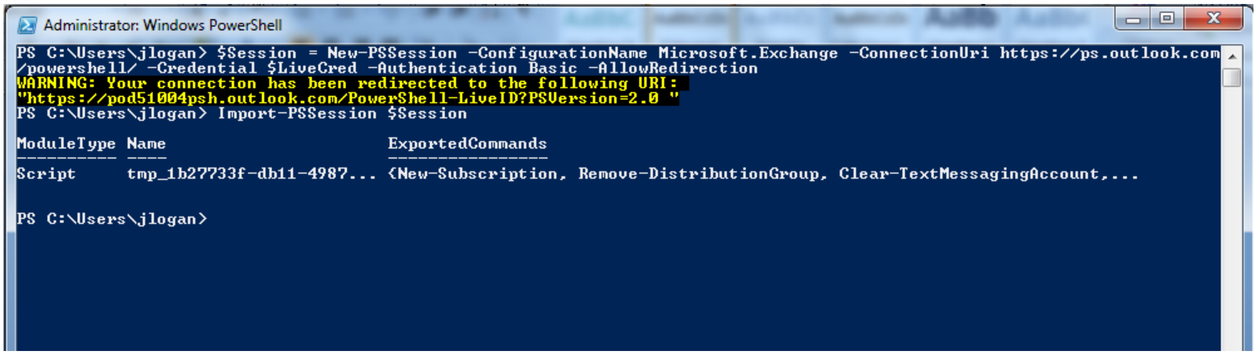
Password: ••••••••••

Next, you will want to create a new session and import that session

Create and Import Session

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.outlook.com/powershell/ -Credential $LiveCred -Authentication Basic -AllowRedirection

Import-PSSession $Session



Administrator: Windows PowerShell

```
PS C:\Users\jlogan> $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.outlook.com
/powershell/ -Credential $LiveCred -Authentication Basic -AllowRedirection
WARNING: Your connection has been redirected to the following URI:
"https://pod51004psh.outlook.com/PowerShell-LiveID?PSVersion=2.0 "
PS C:\Users\jlogan> Import-PSSession $Session

ModuleType Name                      ExportedCommands
---------- ----                      ----------------
Script     tmp_1b27733f-db11-4987... {New-Subscription, Remove-DistributionGroup, Clear-TextMessagingAccount,...


PS C:\Users\jlogan>
```

You are now connected and ready to use PowerShell against your Outlook Live environment. To disconnect once you are finished:

To Disconnect

```
Remove-PSSession $Session
```

When performing any task in PowerShell you should practice utilizing the *get-help* and *get- command* cmdlets for assistance. Use the following syntax to understand all of the parameters associated with PowerShell cmdlets:

Get-Help nameofcmdletyouwanttouse –full

Ex. **Get-Help New-TransportRule -full**

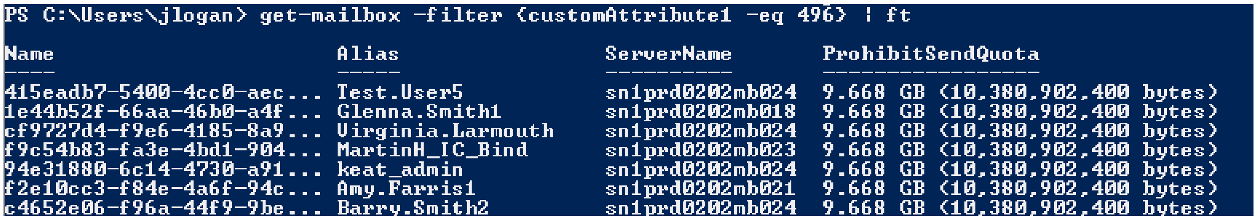
3.6.2 PowerShell – *Examples* – Common Query Tasks

*These task can be performed in either the **Staff** or **Student** Tenant*

The following are some common queries you can perform to get info about mail-enabled objects in your district.

All mailboxes in the district:

Get-mailbox –Filter {customAttribute1 –eq 496} | Format-Table



```
PS C:\Users\jlogan> get-mailbox -filter {customAttribute1 -eq 496} | ft

Name                          Alias                   ServerName         ProhibitSendQuota
----                          -----                   ----------         -----------------
415eadb7-5400-4cc0-aec... Test.User5              sn1prd0202mb024  9.668 GB (10,380,902,400 bytes)
1e44b52f-66aa-46b0-a4f... Glenna.Smith1           sn1prd0202mb018  9.668 GB (10,380,902,400 bytes)
cf9727d4-f9e6-4185-8a9... Virginia.Larmouth       sn1prd0202mb024  9.668 GB (10,380,902,400 bytes)
f9c54b83-fa3e-4bd1-904... MartinH_IC_Bind         sn1prd0202mb023  9.668 GB (10,380,902,400 bytes)
94e31880-6c14-4730-a91... keat_admin              sn1prd0202mb024  9.668 GB (10,380,902,400 bytes)
f2e10cc3-f84e-4a6f-94c... Amy.Farris1             sn1prd0202mb021  9.668 GB (10,380,902,400 bytes)
c4652e06-f96a-44f9-9be... Barry.Smith2            sn1prd0202mb024  9.668 GB (10,380,902,400 bytes)
```

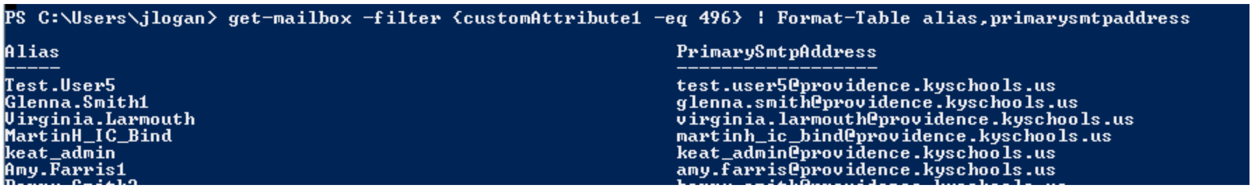
The above example uses OPATH syntax with *customAttribute1*, which is stamped by the provisioning system with the district number, in this case Providence. You could also substitute *customAttribute1* with other attributes if you wish such as *Company* and supply that attribute's value if desired.

Note: If you have more than 1,000 objects returned you will want to add *–resultsize unlimited* to a command:

Get-mailbox –resultsize unlimited –Filter {customAttribute1 –eq 496} | Format-Table

Notice when you run the above command the *Name* value contains the SystemID which is created by OLPS and can be found in ADUC on the KETS EDU tab. Not very helpful for this example, so you could choose to clean the output up using a pipe (|) and the Format-Table cmdlet, specifying only the attributes you'd like to see.

Get-mailbox –Filter {customAttribute1 –eq 496} | Format-Table displayname, primarysmtpaddress

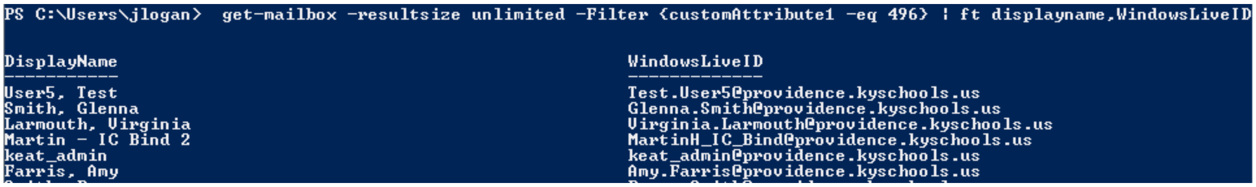


```
PS C:\Users\jlogan> get-mailbox -filter {customAttribute1 -eq 496} | Format-Table alias,primarysmtpaddress

Alias                                                       PrimarySmtpAddress
-----                                                       ------------------
Test.User5                                                  test.user5@providence.kyschools.us
Glenna.Smith1                                               glenna.smith@providence.kyschools.us
Virginia.Larmouth                                           virginia.larmouth@providence.kyschools.us
MartinH_IC_Bind                                             martinh_ic_bind@providence.kyschools.us
keat_admin                                                  keat_admin@providence.kyschools.us
Amy.Farris1                                                 amy.farris@providence.kyschools.us
```

To get a list of all Windows Live IDs that exist for your district you could simply add that attribute:

Get-mailbox –Filter {customAttribute1 –eq 496} | Format-Table displayname, WindowsLiveID

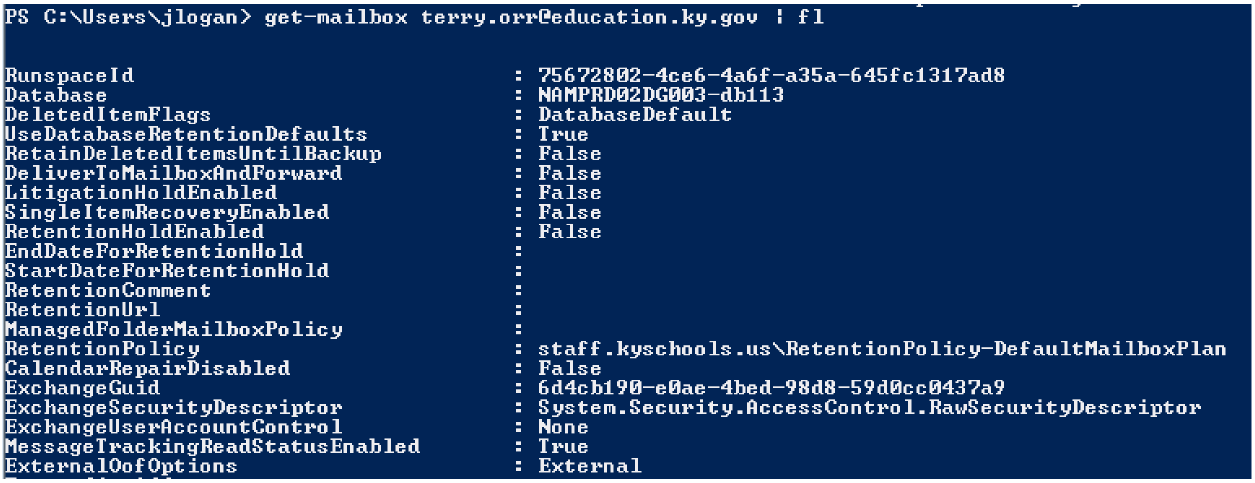


```
PS C:\Users\jlogan>  get-mailbox -resultsize unlimited -Filter {customAttribute1 -eq 496} | ft displayname,WindowsLiveID

DisplayName                                             WindowsLiveID
-----------                                             -------------
User5, Test                                             Test.User5@providence.kyschools.us
Smith, Glenna                                           Glenna.Smith@providence.kyschools.us
Larmouth, Virginia                                      Virginia.Larmouth@providence.kyschools.us
Martin - IC Bind 2                                      MartinH_IC_Bind@providence.kyschools.us
keat_admin                                              keat_admin@providence.kyschools.us
Farris, Amy                                             Amy.Farris@providence.kyschools.us
```

For a list of all available attributes that you may choose to query on like *displayname* and *primarysmtpaddress* used above perform a get-mailbox on an individual mailbox and allow a full list to be displayed. This is accomplished using the Format-List cmdlets instead of Format-Table:

Get-mailbox terry.orr@education.ky.gov | Format-List

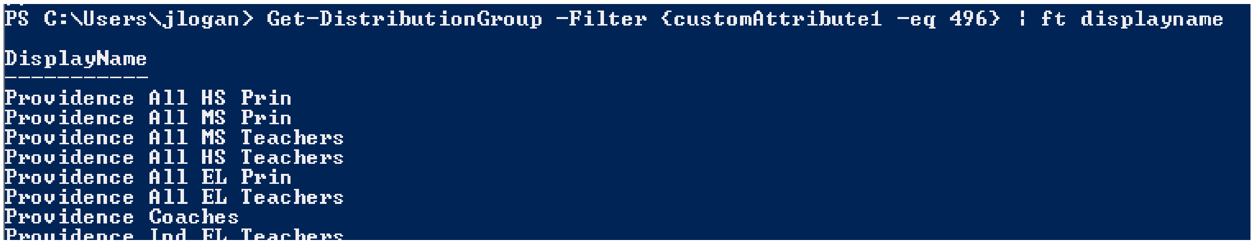


```
PS C:\Users\jlogan> get-mailbox terry.orr@education.ky.gov ¦ fl


RunspaceId                          : 75672802-4ce6-4a6f-a35a-645fc1317ad8
Database                            : NAMPRD02DG003-db113
DeletedItemFlags                    : DatabaseDefault
UseDatabaseRetentionDefaults        : True
RetainDeletedItemsUntilBackup       : False
DeliverToMailboxAndForward          : False
LitigationHoldEnabled               : False
SingleItemRecoveryEnabled           : False
RetentionHoldEnabled                : False
EndDateForRetentionHold             :
StartDateForRetentionHold           :
RetentionComment                    :
RetentionUrl                        :
ManagedFolderMailboxPolicy          :
RetentionPolicy                     : staff.kyschools.us\RetentionPolicy-DefaultMailboxPlan
CalendarRepairDisabled              : False
ExchangeGuid                        : 6d4cb190-e0ae-4bed-98d8-59d0cc0437a9
ExchangeSecurityDescriptor          : System.Security.AccessControl.RawSecurityDescriptor
ExchangeUserAccountControl          : None
MessageTrackingReadStatusEnabled    : True
ExternalOofOptions                  : External
```

To get a list of all Distribution Groups for your district:

Get-DistributionGroup –Filter { customAttribute1 –eq 496} | Format-Table displayname

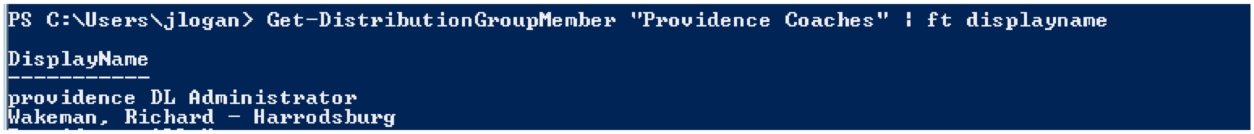


```
PS C:\Users\jlogan> Get-DistributionGroup -Filter {customAttribute1 -eq 496} ¦ ft displayname

DisplayName
-----------
Providence All HS Prin
Providence All MS Prin
Providence All MS Teachers
Providence All HS Teachers
Providence All EL Prin
Providence All EL Teachers
Providence Coaches
Providence Ind EL Teachers
```

To get a list of all members of a Distribution Group you can use the Get-DistributionGroupMember cmdlets:

Get-DistributionGroupMember "Providence Coaches" | Format-Table displayname



```
PS C:\Users\jlogan> Get-DistributionGroupMember "Providence Coaches" ¦ ft displayname

DisplayName
-----------
providence DL Administrator
Wakeman, Richard - Harrodsburg
```

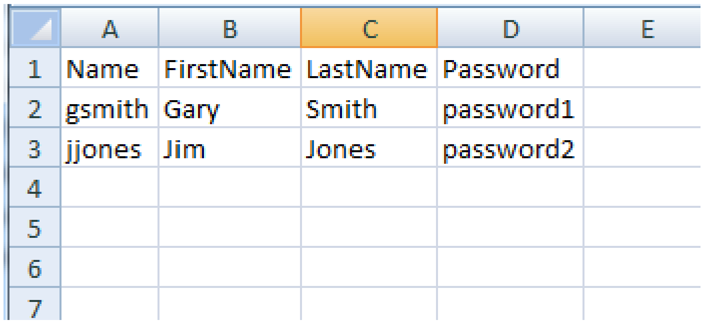
3.6.3 PowerShell – *Example* – Bulk User Creation

*This task can be performed in either the **Staff** or **Student** Tenant.*

You can user PowerShell to batch create users using a CSV. It's important to realize that this would ONLY create Windows Live IDs and mailboxes in Outlook Live. **DO NOT** run PowerShell commands or EWS scripts without a solid understanding and knowing for certain the outcome.

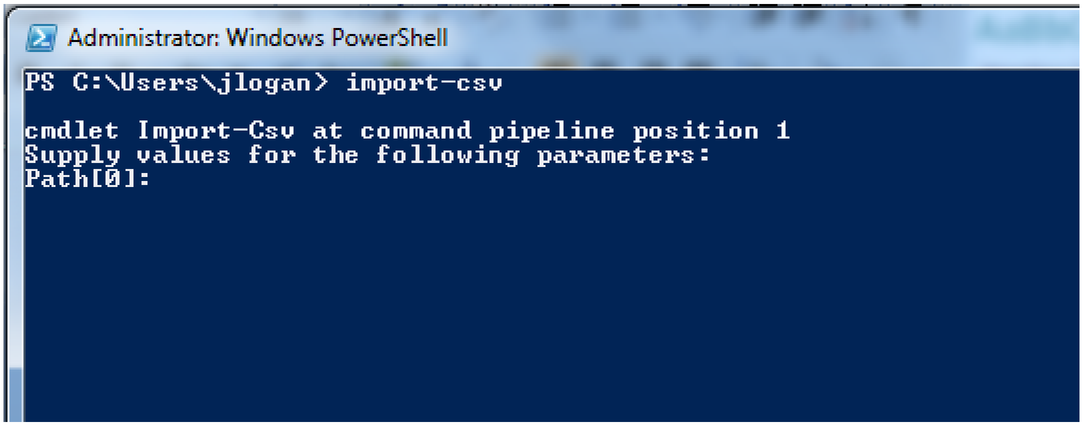
Important Note: This process would NOT create a corresponding Active Directory object. This is merely an example of how you could use PowerShell to create Outlook Live mailboxes for resources like Conference Rooms, Calendars, Distribution Groups, etc that would not need a corresponding user object in Active Directory. Creating users in Active Directory is the mechanism that should be followed for most user operations.

The format of the CSV can simply be as follows: (or you can add supply other attributes as you wish)



	A	B	C	D	E
1	Name	FirstName	LastName	Password	
2	gsmith	Gary	Smith	password1	
3	jjones	Jim	Jones	password2	
4					
5					
6					
7					

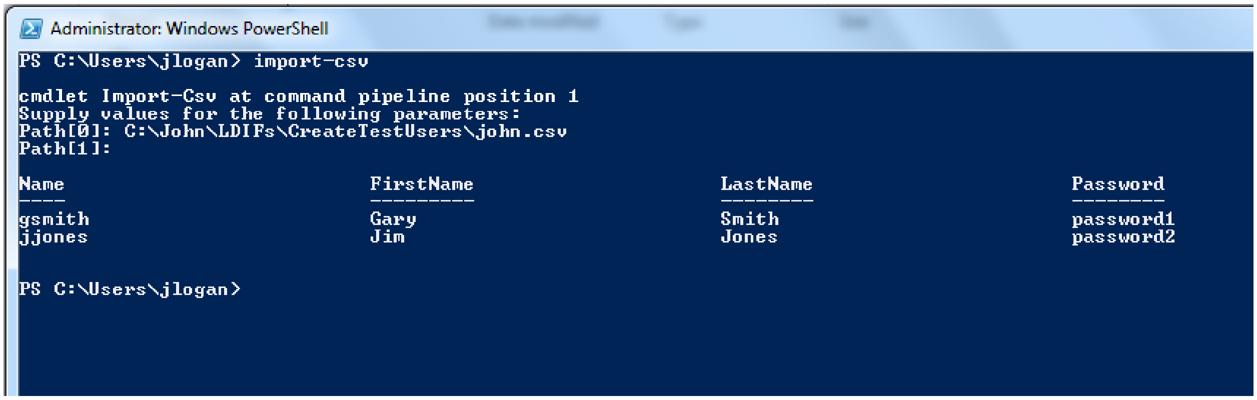
From PowerShell you would simply type Import-CSV and supply the path and filename as shown in the following screenshot. *You must first use the steps detailed in 'PowerShell – Connecting to Outlook Live' above before proceeding.*



```
PS C:\Users\jlogan> import-csv

cmdlet Import-Csv at command pipeline position 1
Supply values for the following parameters:
Path[0]:
```

After entering the path press <*Enter*> again and the CSV should be imported as shown below



```
PS C:\Users\jlogan> import-csv

cmdlet Import-Csv at command pipeline position 1
Supply values for the following parameters:
Path[0]: C:\John\LDIFs\CreateTestUsers\john.csv
Path[1]:

Name                      FirstName                 LastName                  Password
----                      ---------                 --------                  --------
gsmith                    Gary                      Smith                     password1
jjones                    Jim                       Jones                     password2


PS C:\Users\jlogan>
```

You can also do what's called Pipelining. To demonstrate this, take the last example of creating the accounts from the CSV. The process did create the accounts, but did **not** create the password properly as it was not created as a string. This means you must force the values of the password field as a string. To do this you could read the entries from the CSV first, then 'pipe' the values individually through another process. This is done with the '|' key (Hold 'Shift' and hit \ 'Forward Slash' key). You could add to notepad and save with extension .ps1 to run in the future. Ps1 extensions are PowerShell scripts that can be run like a bat, cmd or exe.

Example script

Import-CSV "C:\John\PowerShell\scripts\Providencekyschoolsus_test users.csv" | foreach { $PassW = (get-Mailbox $_.Name).Password Set-Mailbox $_.Name -Password (ConvertTo-SecureString -String 'password' -AsPlainText -Force) -ResetPasswordOnNextLogon 0}

3.6.4 PowerShell – *Example* – Add Secondary Proxy SMTP Address

*This task can be performed in either the **Staff** or **Student** Tenant.*

The following code can be used to create a secondary SMTP address for a given user. This code should be copy/pasted into notepad and saved with any name you wish but should have a .PS1 extension. From a PowerShell command prompt you can simply type the name of the file to run. Edit the second and third lines of the file to give the desired user's login ($user) and then modify the desired secondary Proxy SMTP address ($smtp). *You must first use the steps detailed in 'PowerShell – Connecting to Outlook Live' above before proceeding.*

```
#--Begin Script
#Script to add a secondary SMTP address to a specified user
# Edit the following 2 lines for the mailbox you would like to modify
$user = john.logan@education.ky.gov
$smtp = "mailman@education.ky.gov"

$Mbx = Get-Mailbox -Identity $user
$Found = $false

foreach ($Email in $Mbx.EmailAddresses)
{
   echo $Email
   if ($Email.ToLower().Contains($smtp.ToLower()))
   {
      $Found = $true
   }
}
if (!$Found)
{
   $Mbx.EmailAddresses.Add($smtp)
   Set-Mailbox $user -EmailAddresses $Mbx.EmailAddresses
}
#--End Script
```

3.6.5 PowerShell – *Example* – Set TimeZone for Users

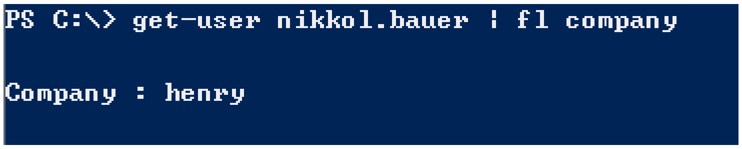
*This task can be performed in either the **Staff** or **Student** Tenant.*

By default the Time Zone and Language are not set on mailbox creation. You may choose to create Staff members and allow them to set their TimeZone/Language upon their first login into OWA, or run the following PowerShell cmdlets to set it each time you create users. Districts will more than likely want to run this cmdlets against the Student Tenant when multiple student objects are created. The cmdlets will set the Time Zone and Language each time its run for all mailboxes, which will not cause any problems.

Note: Use either "Central Standard Time" or "Eastern Standard Time"

Get-User -Filter {company -eq "*district*"} | Set-MailboxRegionalConfiguration -TimeZone "Eastern Standard Time" -Language en-US

where ***district*** is the value of the 'Company' field. To find the value of the 'Company' field you can use the following example:



```
PS C:\> get-user nikkol.bauer ¦ fl company

Company : henry
```

Note: The 'Company' attribute is populated by OLPS and should be set the same for all uses, Staff or Student, in Outlook Live. Regardless of what a district has placed in the 'Company' field in AD for a user, that value does not 'flow' to Outlook Live. A predetermined value is populated in every mail user's 'Company' field in Outlook Live. Ex. 'henry' for Henry County users, 'providence' for all Providence users, etc.

3.6.6 PowerShell – *Example* – Transport Rules

*This task can only be performed in the **Student** Tenant.*

In the Student Tenant you have the ability to modify the behavior of mail flow in and out to your students. This can be done in the Exchange Control Panel but using PowerShell you can create very powerful rules to control the flow of mail.

*Note: use '**Get-Help New-TransportRule –full**' to get a list of the many different scenarios you can create.*

As an example the following PowerShell command would create a Transport Rule called "Unaccepted Domains" which would delete any message destined for any student in the Providence domain that is sent from any mailbox in the domains *company1.com* or *company2.com,* except if the desired student recipient is tommy@providence.kyschools.us

New-TransportRule -Name "Unaccepted Domains" -RecipientAddressMatchesPatterns "@company1.com$,@comany2.com$" -ExceptIfRecipientAddressMatchesPatterns "tommy@providence.kyschools.us$" -DeleteMessage $true

3.6.7 PowerShell – *Example* – Hide Mailbox

Mailboxes can be set to 'hidden' using the KETS EDU tab in ADUC. This will hide the mailbox from being seen in the Global Address List (this is the default behavior for all mailboxes in the Student Tenant). If, during a Active Directory user object deletion you could select the 'Hidden' option in ADUC on the KETS EDU tab, allow that to replicate through the system, then delete the AD object. Or you could choose to run the following PowerShell command against the object.

get-mailbox joe.cool@providence.kyschools.us | set-mailbox -MailboxPlan GalDisabledMailboxPlan

To make the mailbox visible in the GAL again you would change 'GalDisabledMailboxPlan' to 'DefaultMailboxPlan' under the –MailboxPlan parameter.

3.6.8 PowerShell – *Example* – Allow External Sending to Distribution Groups (used for SMTP Relaying to DGs)

*This task can be performed in either the **Staff** or **Student** Tenant.*

In order for applications/devices to relay mail through the SMTP relay servers to a Distribution Group, the Distribution Group must be configured to accept mail from inside AND outside the organization. By default, only senders inside the organization can send to a DG. The following PowerShell cmdlet sets the Distribution Group named 'Providence IT Staff' to accept messages from outside the organization (ex. From an external partner or a device on-premise that relays SMTP mail to the members of the group).

Note: The font size has been reduced to show the cmdlets on one-line.

Set-DistributionGroup ProvidenceITStaff@providence.kyschools.us –RequireSenderAuthenticationEnabled $False

3.6.9 PowerShell – *Example* – Add Mailbox Permissions

*This task can be performed in either the **Staff** or **Student** Tenant.*

The following code can be used to give a user full mailbox permission access to another mailbox. Once this is done you can create a new Outlook profile for this 'second' mailbox and login. *You must first use the steps detailed in 'PowerShell – Connecting to Outlook Live' above before proceeding.*

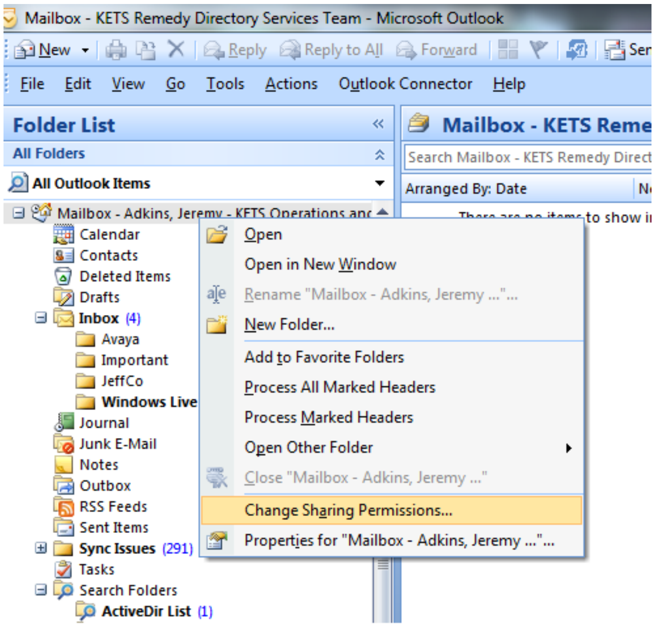
add-MailboxPermission -Identity *targetmailbox* -User *usertogiveaccessto* -AccessRights fullaccess

where *targetmailbox* is the desired mailbox's SMTP address that will be opened and *usertogiveaccessto* is the SMTP address of the user that needs to open the target mailbox.

To open the second mailbox as an additional mailbox from 'your' Outlook profile you would have to first create a profile in Outlook for this second mailbox, login and set Share permissions on each folder that you want to open, giving the desired user access. Then you could open this mailbox as a second mailbox.

Create the profile for the targetmailbox.

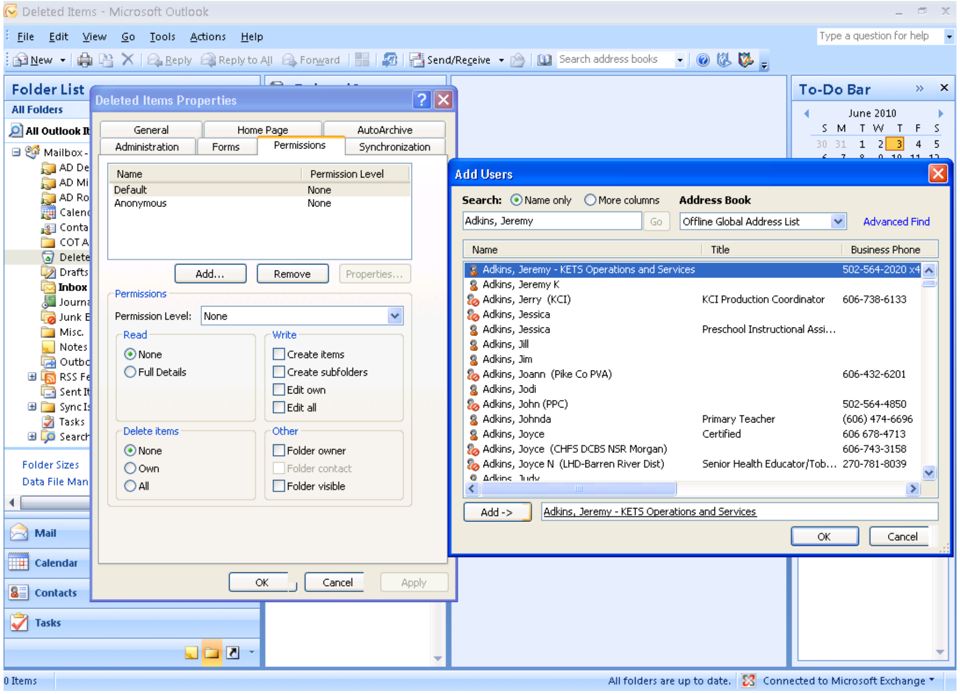
Press Alt + G + L to change the current view to Folder List



Screenshot 1.1

Right Click the top level in the Folder List and click Change Sharing Permissions shown in screenshot 1.1.

Click Add and select the User you want to share the mailbox with. Show in screenshot 1.2.



Deleted Items Properties

General | Home Page | AutoArchive | Administration | Forms | Permissions | Synchronization

Name	Permission Level
Default	None
Anonymous	None

Add... Remove Properties...

Permissions

Permission Level: None

Read: ● None ○ Full Details

Write: □ Create items □ Create subfolders □ Edit own □ Edit all

Delete items: ● None ○ Own ○ All

Other: □ Folder owner □ Folder contact □ Folder visible

OK Cancel Apply

Add Users

Search: ● Name only ○ More columns Address Book

Adkins, Jeremy Go Offline Global Address List Advanced Find

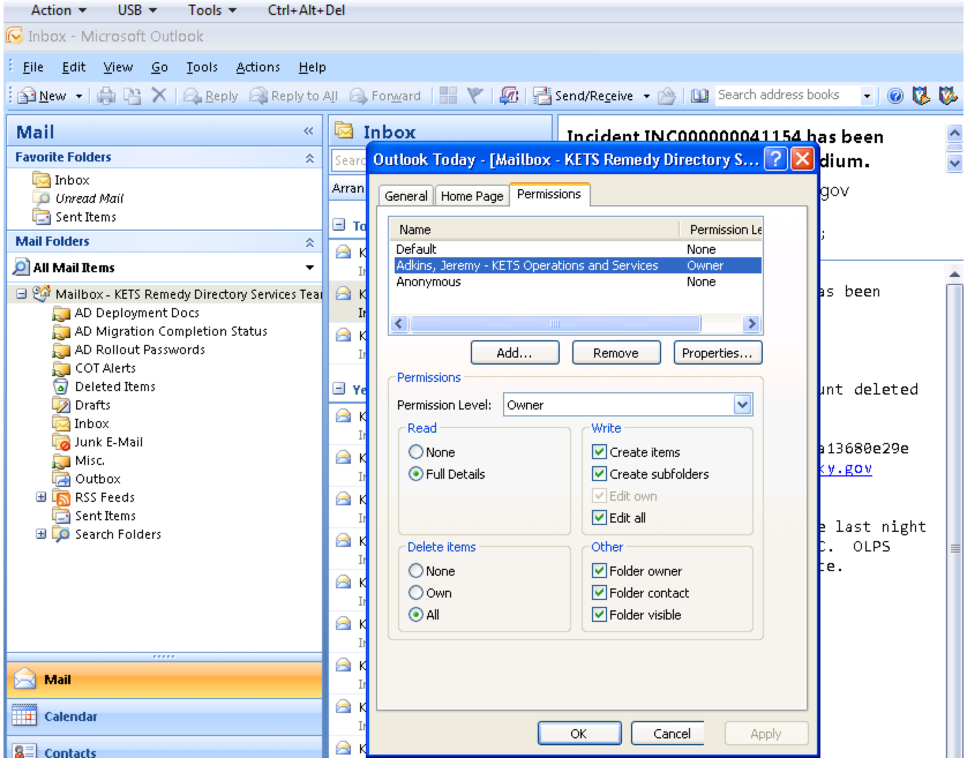
Name	Title	Business Phone
Adkins, Jeremy - KETS Operations and Services		502-564-2020 x4
Adkins, Jeremy K		
Adkins, Jerry (KCI)	KCI Production Coordinator	606-738-6133
Adkins, Jessica		
Adkins, Jessica	Preschool Instructional Assi...	
Adkins, Jill		
Adkins, Jim		
Adkins, Joann (Pike Co PVA)		606-432-6201
Adkins, Jodi		
Adkins, John (PPC)		502-564-4850
Adkins, Johnda	Primary Teacher	(606) 474-6696
Adkins, Joyce	Certified	606 678-4713
Adkins, Joyce (CHFS DCBS NSR Morgan)		606-743-3158
Adkins, Joyce N (LHD-Barren River Dist)	Senior Health Educator/Tob...	270-781-8039
Adkins, Judy		

Add -> Adkins, Jeremy - KETS Operations and Services

OK Cancel

Screenshot 1.2

After adding the user you need to set the appropriate permission level by selecting from the Permission Level: drop down list. For this example I used Owner since the purpose of adding an additional mailbox is usually to manage the mailbox without a need for multiple outlook profiles. It is also possible to set the permission to reviewer (read-only) or any custom combination of permissions. Shown in screenshot 1.3.



Outlook Today - [Mailbox - KETS Remedy Directory S...

General | Home Page | Permissions

Name	Permission Le
Default	None
Adkins, Jeremy - KETS Operations and Services	Owner
Anonymous	None

Add... Remove Properties...

Permissions

Permission Level: Owner

Read
○ None
● Full Details

Write
☑ Create items
☑ Create subfolders
☑ Edit own
☑ Edit all

Delete items
○ None
○ Own
● All

Other
☑ Folder owner
☑ Folder contact
☑ Folder visible

OK Cancel Apply

Screenshot 1.3

Important: This process must be followed for each sub-folder that needs to show up when you add this mailbox as an additional mailbox in Outlook 2007.

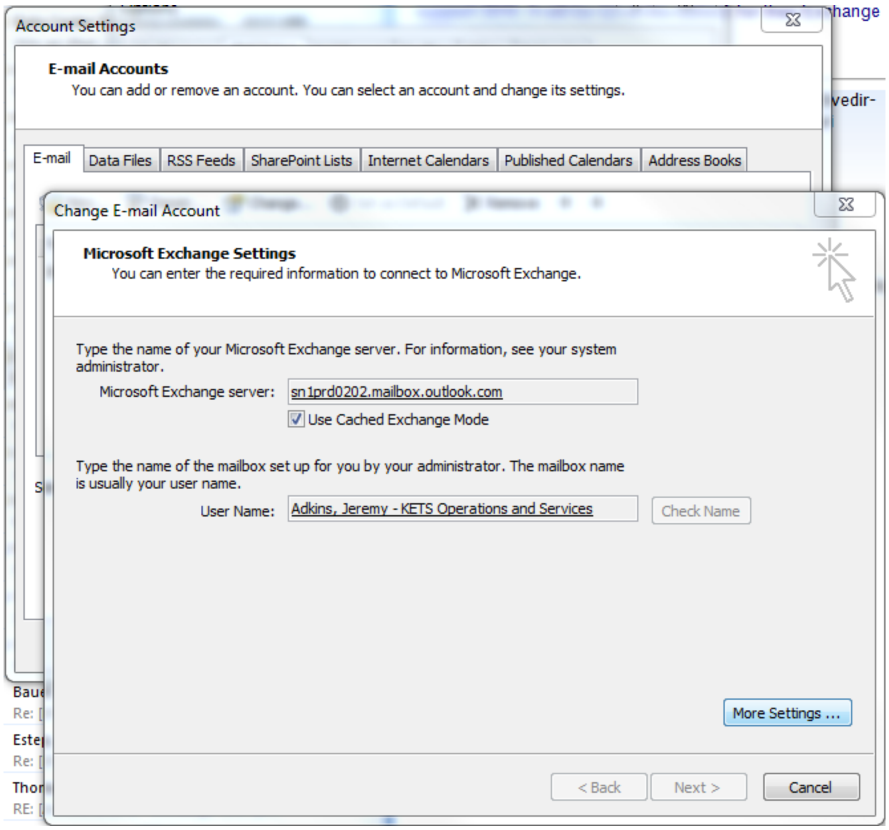
After completing these steps for each user that will need to add the mailbox in Outlook 2007 you can remove the profile for the new mailbox.

Add the new mailbox to Outlook 2007 under an existing profile.

Click Tools -> Options -> Mail Setup tab -> E-mail Accounts

On the Account Settings page make sure the current mailbox is highlighted and select Change.

On the Change E-mail Account page select More Settings. Show in Screenshot 1.4.



E-mail Accounts

You can add or remove an account. You can select an account and change its settings.

Microsoft Exchange Settings

You can enter the required information to connect to Microsoft Exchange.

Type the name of your Microsoft Exchange server. For information, see your system administrator.

Microsoft Exchange server: sn1prd0202.mailbox.outlook.com

☑ Use Cached Exchange Mode

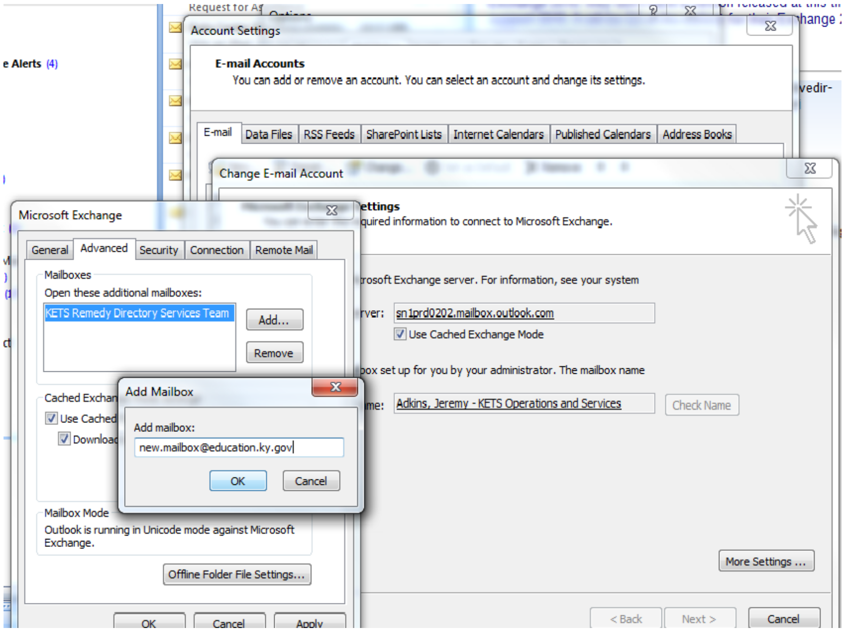
Type the name of the mailbox set up for you by your administrator. The mailbox name is usually your user name.

User Name: Adkins, Jeremy - KETS Operations and Services

Screenshot 1.4

After clicking more settings select the Advanced tab then click Add in the Open these additional mailboxes control. Enter the smtp address of the mailbox you need to add and click ok. Shown in screenshot 1.5.

After adding the new mailbox click ok -> next -> finish -> close -> ok



E-mail Accounts
You can add or remove an account. You can select an account and change its settings.

…ettings
…quired information to connect to Microsoft Exchange.

…rosoft Exchange server. For information, see your system

…rver: sn1prd0202.mailbox.outlook.com
☑ Use Cached Exchange Mode

…box set up for you by your administrator. The mailbox name

…me: Adkins, Jeremy - KETS Operations and Services

Microsoft Exchange

Mailboxes
Open these additional mailboxes:
KETS Remedy Directory Services Team

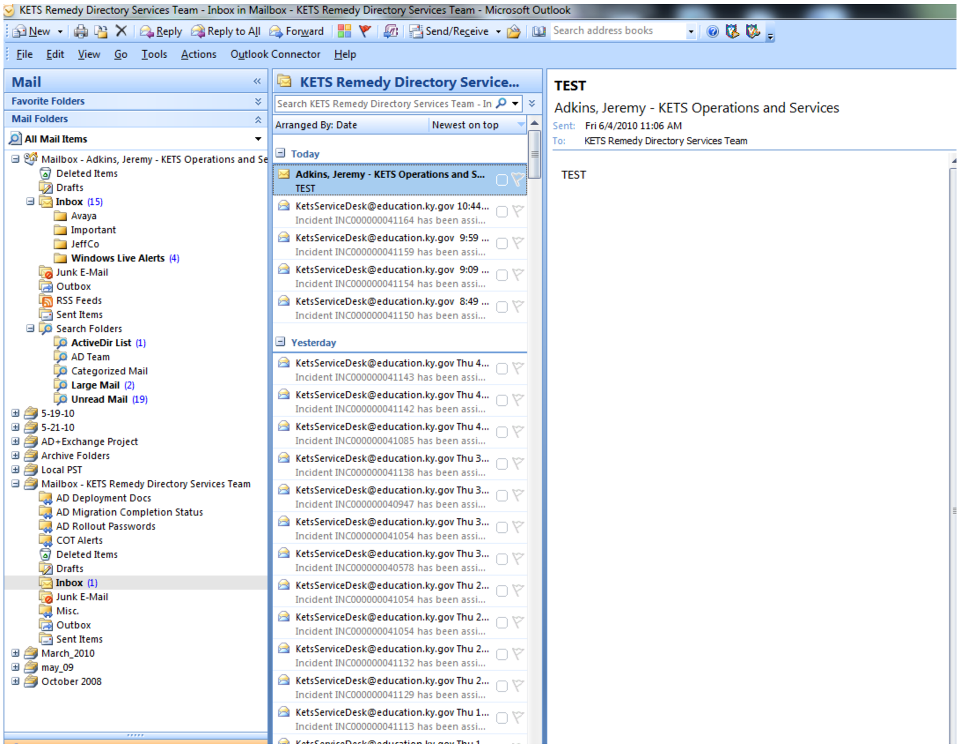
Cached Exchan…
☑ Use Cached
☑ Download

Mailbox Mode
Outlook is running in Unicode mode against Microsoft Exchange.

Add Mailbox
Add mailbox:
new.mailbox@education.ky.gov
OK Cancel

Screenshot 1.5

Now you should see the new mailbox in the Folder List or Mail view along with your current mailbox and any connect PST files. Shown in screenshot 1.6



KETS Remedy Directory Services Team - Inbox in Mailbox - KETS Remedy Directory Services Team - Microsoft Outlook

All Mail Items
- Mailbox - Adkins, Jeremy - KETS Operations and Se…
  - Deleted Items
  - Drafts
  - Inbox (15)
    - Avaya
    - Important
    - JeffCo
    - Windows Live Alerts (4)
  - Junk E-Mail
  - Outbox
  - RSS Feeds
  - Sent Items
  - Search Folders
    - ActiveDir List (1)
    - AD Team
    - Categorized Mail
    - Large Mail (2)
    - Unread Mail (19)
- 5-19-10
- 5-21-10
- AD+Exchange Project
- Archive Folders
- Local PST
- Mailbox - KETS Remedy Directory Services Team
  - AD Deployment Docs
  - AD Migration Completion Status
  - AD Rollout Passwords
  - COT Alerts
  - Deleted Items
  - Drafts
  - Inbox (1)
  - Junk E-Mail
  - Misc.
  - Outbox
  - Sent Items
- March_2010
- may_09
- October 2008

KETS Remedy Directory Service…
Search KETS Remedy Directory Services Team - In…

Today
Adkins, Jeremy - KETS Operations and S… TEST
KetsServiceDesk@education.ky.gov 10:44… Incident INC000000041164 has been assi…
KetsServiceDesk@education.ky.gov 9:59 … Incident INC000000041159 has been assi…
KetsServiceDesk@education.ky.gov 9:09 … Incident INC000000041154 has been assi…
KetsServiceDesk@education.ky.gov 8:49 … Incident INC000000041150 has been assi…

Yesterday
KetsServiceDesk@education.ky.gov Thu 4… Incident INC000000041143 has been assi…
KetsServiceDesk@education.ky.gov Thu 4… Incident INC000000041142 has been assi…
KetsServiceDesk@education.ky.gov Thu 4… Incident INC000000041085 has been assi…
KetsServiceDesk@education.ky.gov Thu 3… Incident INC000000041138 has been assi…
KetsServiceDesk@education.ky.gov Thu 3… Incident INC000000040947 has been assi…
KetsServiceDesk@education.ky.gov Thu 3… Incident INC000000041054 has been assi…
KetsServiceDesk@education.ky.gov Thu 3… Incident INC000000040578 has been assi…
KetsServiceDesk@education.ky.gov Thu 2… Incident INC000000041054 has been assi…
KetsServiceDesk@education.ky.gov Thu 2… Incident INC000000041054 has been assi…
KetsServiceDesk@education.ky.gov Thu 2… Incident INC000000041132 has been assi…
KetsServiceDesk@education.ky.gov Thu 2… Incident INC000000041129 has been assi…
KetsServiceDesk@education.ky.gov Thu 1… Incident INC000000041113 has been assi…

TEST
Adkins, Jeremy - KETS Operations and Services
Sent: Fri 6/4/2010 11:06 AM
To: KETS Remedy Directory Services Team

TEST

Screenshot 1.6

3.6.10 PowerShell – *Example* - Multi-Mailbox Search (aka Cross-Mailbox Search)

*This task can be performed in either the **Staff** or **Student** Tenant.*

District IT staff have the ability to perform what is known as 'multi-mailbox' searching. This is similar to doing an exmerge in the past against Exchange 5.5 or 2003 in which an admin wanted to find messages in user's mailboxes that matched a given criteria. This can be performed across all Staff mailboxes in a district or Student mailboxes.

For Staff, Multi-Mailbox searching is only available through Windows PowerShell. The PowerShell commands must be run with the credentials SearchAdmin@*district*.kyschools.us, where district is the district SMTP Domain Name. The results can be exported to a mailbox of your choosing in the district, such as a District Support Admin mailbox.

The example below would pull all e-mails containing the word 'Test' from all mailboxes in Providence (because they happen to all be members of the EveryoneDL in this example), and would export those messages to the BobAdmin account.

New-MailboxSearch -Name 'Search1' -SearchQuery 'Test' -MessageTypes Email -IncludeUnsearchableItems -LogLevel Basic -SourceMailboxes 'EveryoneDL@providence.kyschools.us' -TargetMailbox 'bob.admin@providence.kyschools.us'

Once the inspection is complete AND the 'exported' information has been copied to another location from the exported folder in the target mailbox (or it is no longer needed) you should delete the MailboxSearch. It is important to understand that deleting the MailboxSearch will also purge the 'results' that were exported to the SearchResults mailbox.

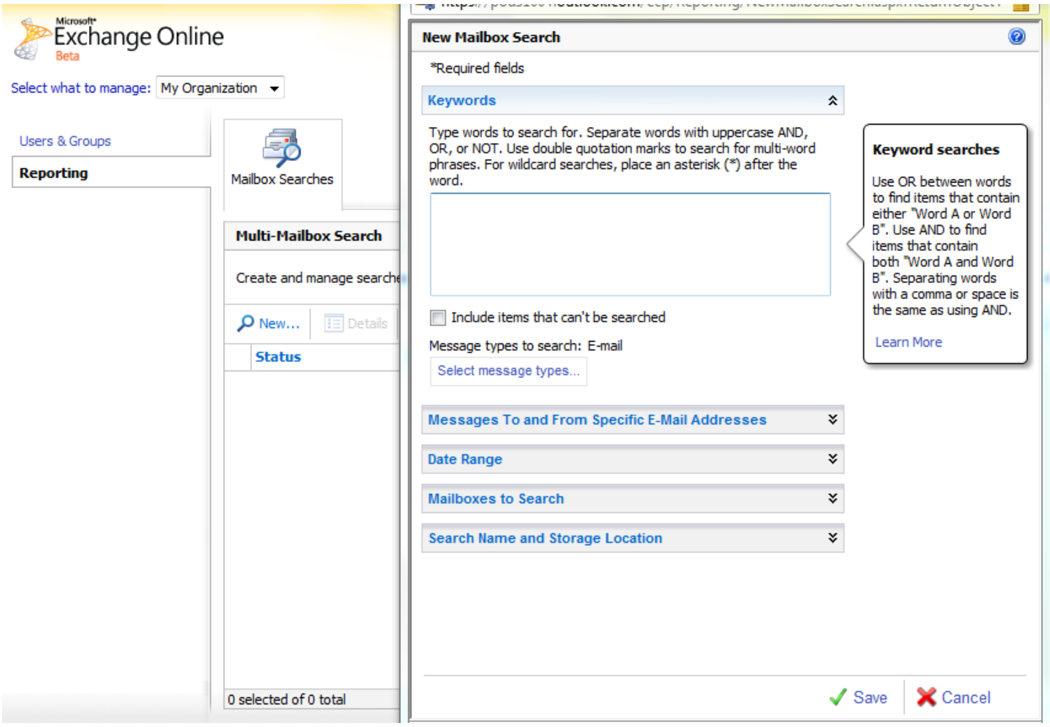
To delete the MailboxSearch when you are completely finished with the exported information run the following command:

Remove-MailboxSearch –Identity 'Search1'

Or whatever the name of the search was that you specified ('Search1' in this example).

For further assistance on how to perform a search using PowerShell: http://technet.microsoft.com/en-us/library/dd298064.aspx

For Students, Multi-Mailbox searching is available through the Exchange Control Panel or through PowerShell. You must be logged in as SearchAdmin@stu.*district*.kyschools.us, where district is the district SMTP Domain Name. The results are exported to a mailbox called SearchResults@stu.district.kyschools.us. The SearchAdmin account has access to open the corresponding SearchResults mailbox for inspection. This can be done through OWA by choosing 'open another user's inbox', or by PowerShell.



Type words to search for. Separate words with uppercase AND, OR, or NOT. Use double quotation marks to search for multi-word phrases. For wildcard searches, place an asterisk (*) after the word.

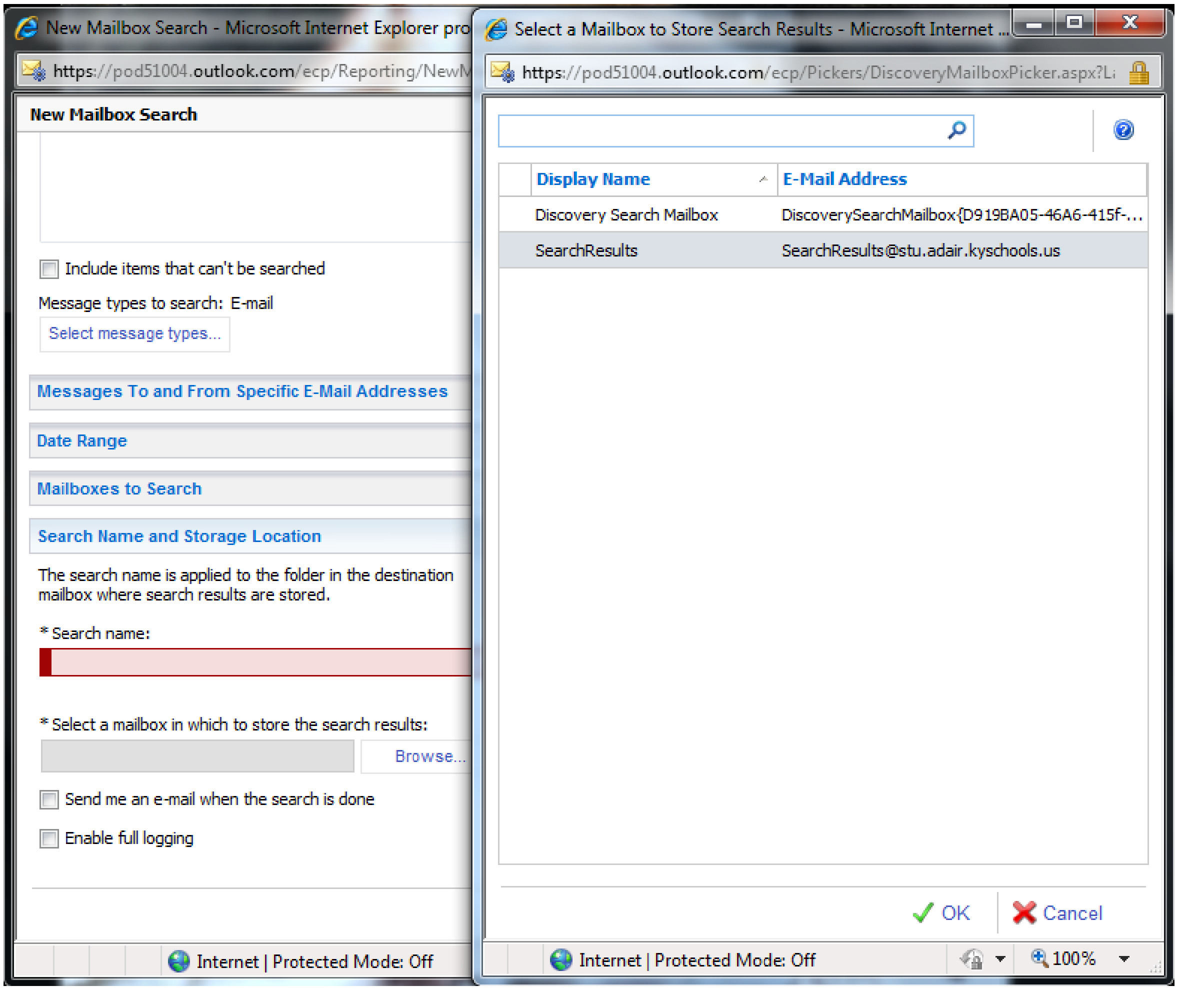
□ Include items that can't be searched

Message types to search: E-mail

Keyword searches

Use OR between words to find items that contain either "Word A or Word B". Use AND to find items that contain both "Word A and Word B". Separating words with a comma or space is the same as using AND.

As you will see there are many settings which can be applied. The one configuration that MUST be set is the ‘Search Name and Location’ on the last option. As shown below you must select ‘Browse’ under *Search Name and Storage Location* to select the SearchResults mailbox. Also type a ‘Search name’ which will be used to create subfolders under the Inbox in the SearchResults mailbox. Under this folder there will be subfolders for each mailbox that matches the criteria.


New Mailbox Search - Microsoft Internet Explorer pro
https://pod51004.outlook.com/ecp/Reporting/NewM
New Mailbox Search
Include items that can't be searched
Select message types...
Messages To and From Specific E-Mail Addresses
Date Range
Mailboxes to Search
Search Name and Storage Location
Browse...
Send me an e-mail when the search is done
Enable full logging
Internet | Protected Mode: Off
Select a Mailbox to Store Search Results - Microsoft Internet ...
https://pod51004.outlook.com/ecp/Pickers/DiscoveryMailboxPicker.aspx?L
OK
Cancel
Internet | Protected Mode: Off
100%

□ Include items that can't be searched

Message types to search: E-mail

The search name is applied to the folder in the destination mailbox where search results are stored.

* Search name:

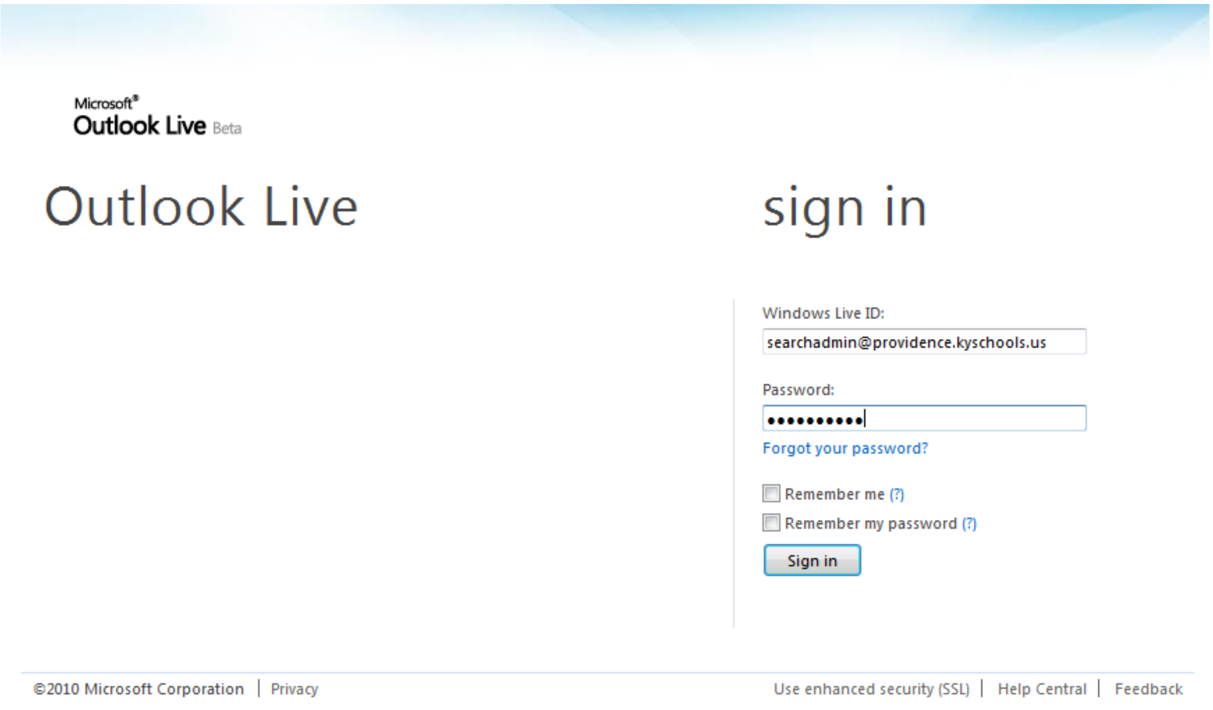
* Select a mailbox in which to store the search results:

□ Send me an e-mail when the search is done

□ Enable full logging

Display Name	E-Mail Address
Discovery Search Mailbox	DiscoverySearchMailbox{D919BA05-46A6-415f-...
SearchResults	SearchResults@stu.adair.kyschools.us

To access the results of the search login as the appropriate SearchAdmin account

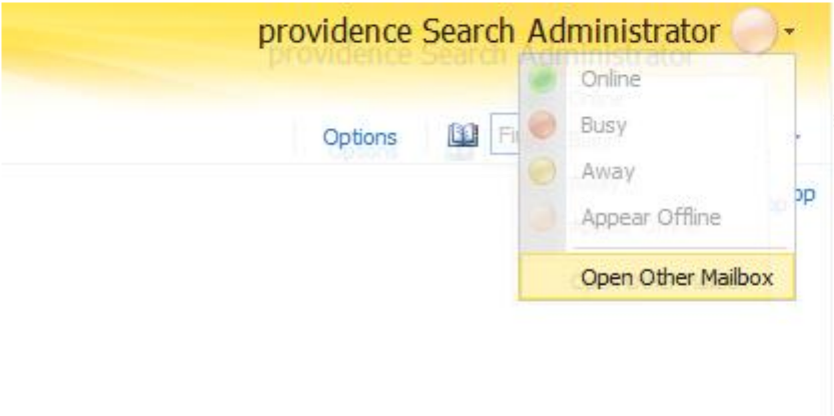

Microsoft®
Outlook Live Beta
Outlook Live
sign in

Windows Live ID: searchadmin@providence.kyschools.us

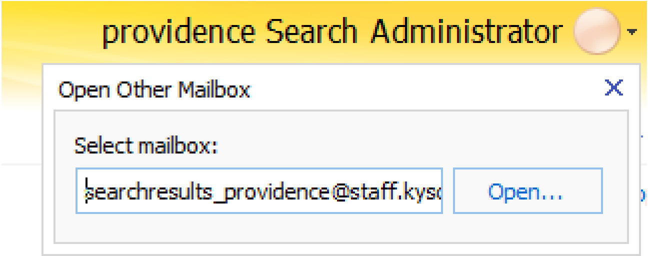
Password: ●●●●●●●●●●

Forgot your password?
□ Remember me (?)
□ Remember my password (?)
Sign in
©2010 Microsoft Corporation | Privacy
Use enhanced security (SSL) | Help Central | Feedback

From the top-right of the page select the drop-down by the presence indicator and select ‘Open Other Mailbox’



Then type the corresponding SearchResults mailbox to open


providence Search Administrator
Open Other Mailbox
Select mailbox:
searchresults_providence@staff.kysc
Open...

3.6.11 PowerShell – *Example* – Create Contact

*This task can be performed in either the **Staff** or **Student** Tenant.*

Mail contacts can be created in Active Directory if desired, but they can also be created directly in Outlook Live using PowerShell. For the Student Tenant this can be accomplished using the GUI as well (in Exchange Control Panel).

To create a mail contact use the following example:

New-Mailcontact -Name "Smith, Bob – CompanyA" -ExternalEmailAddress "bob.smith@companya.com"

3.6.12 PowerShell – *Example* – Add Member to Distribution Group

*This task can be performed in either the **Staff** or **Student** Tenant.*

Group membership can be updated in Active Directory if a corresponding group exists, or using the Exchange Control Panel. However, some groups, such as the "Notifications" DG must be updated using PowerShell.

To update Distribution Group membership, use the following examples:

Add-DistributionGroupMember Notifications@providence.kyschools.us -Member joe.cool@providence.kyschools.us –BypassSecurityGroupManagerCheck

Remove-DistributionGroupMember Notifications@providence.kyschools.us -Member joe.cool@providence.kyschools.us –BypassSecurityGroupManagerCheck

3.6.13 PowerShell – *Example* – Create Dynamic Distribution Groups

*This task can be performed in either the **Staff** or **Student** Tenant.*

For example, the following will create a DDG named "Providence Staff" with SMTP address provstaff@providence.kyschools.us that only includes members with CustomAttribute1 set to "496".

New-DynamicDistributionGroup –Name "Providence Staff" –PrimarySmtpAddress provstaff@providence.kyschools.us –IncludedRecipients MailboxUsers –ConditionalCustomAttribute1 "496"

4 Group Policy

4.1 Overview of Group Policy (GPO)

Group Policy is a feature of Microsoft Windows NT family of operating systems. It is what provides the centralized management and configuration of computers and remote users in an Active Directory environment. In other words, it controls what users can and can't do on a computer network. Although Group Policy is usually used in enterprise environments, its usage is also common in schools, businesses, and other small organizations to restrict certain actions that may pose potential security risks: for instance, blocking the Windows Task Manager, restricting access to certain folders, disabling downloaded executable files and so on.

As part of Microsoft's technologies, it aims to reduce the overall cost of supporting users of Windows. These technologies relate to the management of disconnected machines or roaming users and include Roaming user profiles, Folder redirection and Offline Files.

Helpful Links

Microsoft Windows Group Policy webpage:
http://technet.microsoft.com/en-us/windowsserver/grouppolicy/default.aspx

Microsoft TechNet Group Policy Preferences: Getting Started Guide:http://technet.microsoft.com/en-us/library/cc731892.aspx

Microsoft Learning- Windows Group Policy Resource Kit: Windows Server 2008 and Vista:http://www.microsoft.com/learning/en/us/book.aspx?ID=9556&locale=en-us

4.2 Group Policy Preferences

Windows Server 2008 Domain Services has a new feature called Group Policy Preferences. Group Policy Preferences , which are not ‘required’ policies, but settings which end users can choose to apply or not. The main difference between Group Policies and Group Policy Preferences is how they are enforced (or not enforced).

The table below was pulled from the ‘Group Policy Overview’ document. Group Policy Preferences allow for users of the policies to have flexibility on whether they want the policy applied or not.

	Group Policy Preferences	**Group Policy Settings**
Enforcement	• Preferences are not enforced • User interface is not disabled • Can be refreshed or applied once	• Settings are enforced • User interface is disabled • Settings are refreshed

	Group Policy Preferences	Group Policy Settings
Flexibility	• Easily create preference items for registry settings, files, and so on • Import individual registry settings or entire registry branches from a local or a remote computer	• Adding policy settings requires application support and creating administrative templates • Cannot create policy settings to manage files, folders, and so on
Local Policy	• Not available in local Group Policy	• Available in local Group Policy
Awareness	• Supports non-Group Policy-aware applications	• Requires Group Policy-aware applications
Storage	• Original settings are overwritten • Removing the preference item does not restore the original setting	• Original settings are not changed • Stored in registry Policy branches • Removing the policy setting restores the original settings
Targeting and Filtering	• Targeting is granular, with a user interface for each type of targeting item • Supports targeting at the individual preference item level	• Filtering is based on Windows Management Instrumentation (WMI) and requires writing WMI queries • Supports filtering at a GPO level
User Interface	• Provides a familiar, easy-to-use interface for configuring most settings	• Provides an alternative user interface for most policy settings

For more information on Group Policy Preferences please refer to:

http://www.microsoft.com/DownLoads/details.aspx?familyid=42E30E3F-6F01-4610-9D6E-F6E0FB7A0790&displaylang=en

http://technet.microsoft.com/en-us/library/cc731892(WS.10).aspx

4.3 Group Policy Management Console (GPMC)

GPMC simplifies the management of Group Policy by making it easier to understand, deploy, manage, and troubleshoot Group Policy implementations. GPMC also enables automation of Group Policy operations via scripting.

Just as in Windows Server 2003, GPMC can be used to manage Windows Server 2008 Group Policy implementations. Customers who have at least one valid license of Windows Server 2008 can obtain and use an unlimited number of copies of GPMC. Please see the End User License Agreement (EULA) provided with the GPMC software for details on licensing terms

Installation instructions for Windows XP Professional (GPMC)

1. http://www.microsoft.com/DOWNLOADS/details.aspx?FamilyID=0a6d4c24-8cbd-4b35-9272-dd3cbfc81887&displaylang=en

2. Click the **DOWNLOAD** link to start the download.
3. To Install the GPMC, run the gpmc.msi package. After you accept the End User License Agreement (EULA), all necessary files are installed to the “%Program Files%\GPMC” folder.
4. Prior to starting and using the GPMC, please be sure to read the release notes RelNotes.rtf, which is located in the %Program Files%\GPMC" folder.
5. After installation of the GPMC, you can open the snap-in using either of the following methods:
    - You can open the pre-configured GPMC.msc file. To do this, click **Start**, click **Run**, type **GPMC.msc** and then choose OK. Alternatively, click the **Group Policy Management** shortcut in the **Administrative Tools** folder from the Control Panel.
    - You can create a custom MMC console that contains the GPMC snap-in. To do this:
        1. Open MMC, by clicking **Start**, clicking **Run**, typing **MMC**, and then clicking **OK**.
        2. From the **File** menu, choose **Add/Remove Snap-in**, and then click **Add**.
        3. In the **Add Standalone Snap-in** dialog box, select **Group Policy Management** and click **Add**.
        4. Click **Close**, and then **OK**.

Installation instructions for Windows Vista SP1 Users (RSAT)

1. http://support.microsoft.com/kb/941314
2. Download the RSAT package (32 or 64 bit)
3. Click “**CONTINUE**” to Validate your copy of Windows Vista
4. Double-click the downloaded package to start the Setup wizard. Follow the instructions in the wizard to complete the installation.
5. Open **Control Panel**, click **Programs**, and then click **Turn Windows features on or off** under **Programs and Features**.

    If you are prompted to provide permission by User Account Control, click **Continue**.
6. In the **Windows Features** dialog box, select the remote administration snap-ins and tools that you want to install, and then click **OK**.
7. Configure the Start menu to display the Administration Tools shortcut. To do this, follow these steps:
    a. Right-click **Start**, and then click **Properties**.
    b. On the **Start Menu** tab, click **Customize**.
    c. In the **Customize Start Menu** dialog box, scroll down to **System administrative tools**, and then select **Display on the All Programs menu and the Start menu**.
    d. Click **OK**.

4.4 Delegated Permissions

Your Group Policy design will probably call for delegating certain Group Policy administrative tasks. Determining to what degree to centralize or distribute administrative control of Group Policy is one of the most important factors to consider when assessing the needs of your organization

You can delegate the following Group Policy tasks:

- Creating GPOs
- Managing individual GPOs (for example, granting Edit or Read access to a GPO)
- Performing the following tasks on sites and OUs:
    - Managing Group Policy links for a given site or OU
    - Performing Group Policy Modeling analyses for objects in that container (not applicable for sites)
    - Reading Group Policy Results data for objects in that container (not applicable for sites)
- Creating WMI filters
- Managing and editing individual WMI filters

Delegating management of individual GPOs

Using GPMC, you can easily grant additional users permissions on a GPO. GPMC manages permissions at the task level. There are five levels of allowed permissions on a GPO: Read, Edit, and Edit/Delete/Modify Security, Read (from Security Filtering), and Custom. These permission levels correspond to a fixed set of low-level permissions.

GPO Permission Options

Read	Allow Read Access on the GPO
Read (from Security Filterting)	This setting cannot be set directly, but appears if the user has Read and Apply Group Policy permissions to the GPO, which is set using Security Filtering on the **Scope** tab of the GPO
Edit settings	Allow Read, Write, Create Child Objects, Delete Child Objects
Edit, delete and modify security	Allow Read, Write, Create Child Objects, Delete Child Objects, Delete, Modify Permissions, and Modify Owner. This is essentially **FULL CONTROL** without the Apply Group Permission set.
Custom	Any other combination of rights. You cannot set these by clicking **ADD**, they can only be set using the ACL editor directly, which can be accessed by clicking **ADVANCED**.

You can click **Add** to grant users permissions on a GPO. This starts the object picker so you can find the desired user or group to set the permission level. You can then set the permission level by selecting the **Read**, **Edit**, or **Edit, Delete, Modify Security** permissions.

Note that the **Apply Group Policy** permission, which is used for Security Filtering, cannot be set using the **Delegation** tab. Because setting **Apply Group Policy** is used for scoping the GPO, this permission is managed on the **Scope** tab of the GPMC user interface. When you grant a user Security Filtering on the **Scope** tab, you are actually setting both the **Read** and **Apply Group Policy** permissions.

To delegate Group Policy administrative tasks on a container

1. To delegate Group Policy-related permission on an OU, click the appropriate container in the GPMC console.
2. In the right pane for the OU, click the **Delegation** tab.
3. In the drop-down list box, select the desired permission you want to manage: **Link GPOs**, **Perform Group Policy Modeling analyses**, or **Read Group Policy Results data**. To add new groups, use the **Add** button.
4. To modify the **Applies To** setting for an existing permission, right-click the user or group in the list and then select either **This container only** or **This container and all child containers**.
5. To remove an existing group or user from having the specified permission, select the user or group from the list and click the **Remove** button. Only domain administrators have permission to do this.
6. To add or remove custom permissions, click **Advanced** at the bottom-right of the details pane and select the object whose permissions you want to change. Note that setting custom permissions is *not* recommended.

Delegating Creation of GPOs

The ability to create GPOs in a domain is a permission that is managed on a per-domain basis. By default, only Domain Administrators, Enterprise Administrators, Group Policy Creator Owners, and SYSTEM can create new Group Policy objects. If the domain administrator wants a non-administrator or non-administrative group to be able to create GPOs, that user or group can be added to the Group Policy Creator Owners security group. Alternatively, you can use the **Delegation** tab on the Group Policy Objects container in GPMC to delegate creation of GPOs. When a non-administrator who is a member of the Group Policy Creator Owners group creates a GPO, that user becomes the creator owner of the GPO and can edit the GPO and modify permissions on the GPO. However, members of the Group Policy Creator Owners group cannot link GPOs to containers unless they have been separately delegated the right to do so on a particular site, domain, or OU. Being a member of the Group Policy Creator Owners group gives the non-administrator full control of only those GPOs that the user creates. Group Policy Creator Owner members do not have permissions for GPOs that they do not create.

Note

- When an administrator creates a GPO, the Domain Administrators group becomes the Creator Owner of the Group Policy object. By default, Domain Administrators can edit all GPOs in the domain.

The right to link GPOs is delegated separately from the right to create GPOs and the right to edit GPOs. Be sure to delegate both rights to those groups you want to be able to create and link GPOs. By default, non-Domain Admins cannot manage links, and this prevents them from being able to use GPMC to create and link a GPO. However, non-Domain Admins can create an unlinked GPO if they are members of the **Group Policy Creator Owners** group. After a non-Domain Admin creates an unlinked GPO, the Domain Admin or someone else who has been delegated permissions to link GPOs an a container can link the GPO as appropriate.

Creation of GPOs can be delegated to any group or user. There are two methods of granting a group or user this permission:

- Add the group or user to the Group Policy Creator Owners group. This was the only method available prior to GPMC.
- Explicitly grant the group or user permission to create GPOs. This method is newly available with GPMC.

You can manage this permission by using the **Delegation** tab on the Group Policy objects container for a given domain in GPMC. This tab shows the groups that have permission to create GPOs in the domain, including the Group Policy Creator Owners group. From this tab, you can modify the membership of existing groups that have this permission, or add new groups.

Because the Group Policy Creator Owners group is a domain global group, it cannot contain members from outside the domain. Being able to grant users permissions to create GPOs without using Group Policy Creator Owners facilitates delegating GPO creation to users outside the domain. Without GPMC, this task cannot be delegated to members outside the domain.

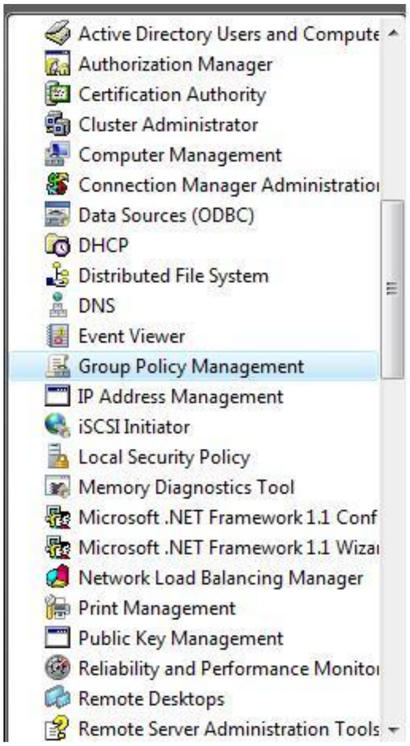
If you require that users outside the domain have the ability to create GPOs, create a new domain local group in the domain (for example, "GPCO – External"), grant that group GPO creation permissions in the domain, and then add domain global groups from external domains to that group. For users and groups in the domain, you should continue to use the Group Policy Creator Owners group to grant GPO-creation permissions.

Adding a user to the membership of Group Policy Creator Owners and granting the user GPO-creation permissions directly using the new method available in GPMC are identical in terms of permissions.

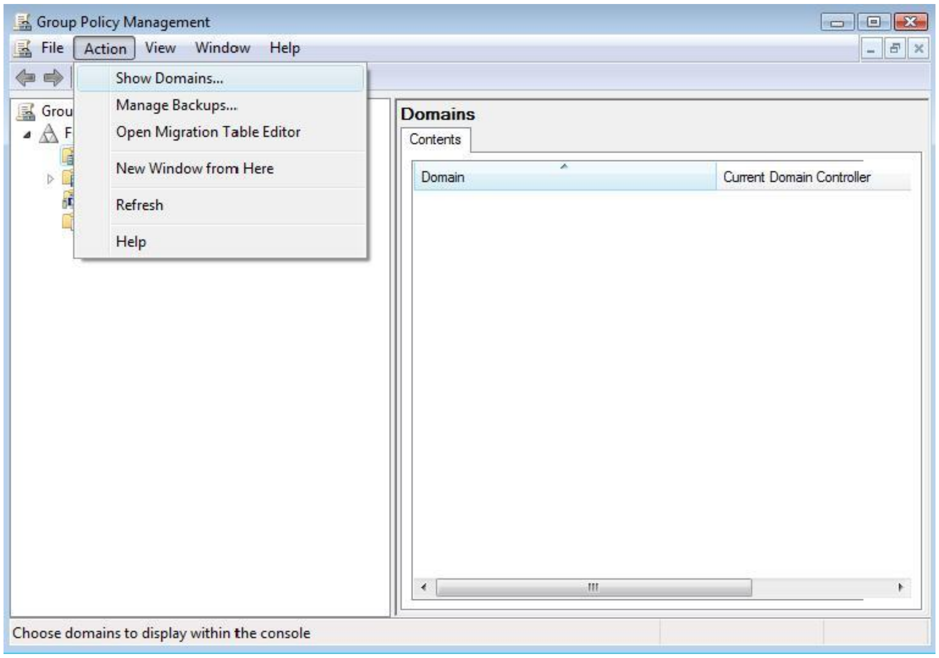
4.5 Most Popular Policy Questions

1. How to create and link a Group Policy using GPMC

1. **Open Group Policy Management.**



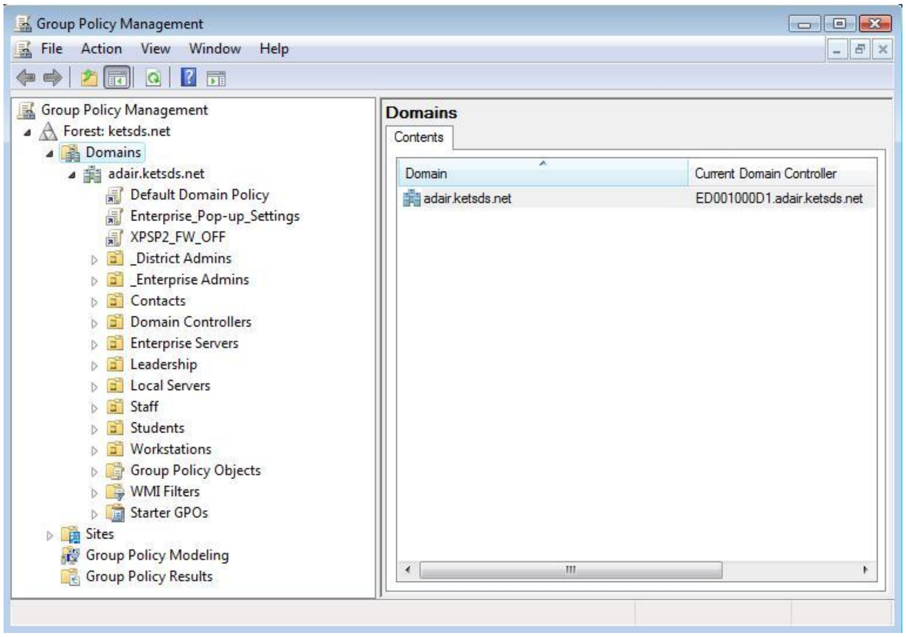
2. Click Action and show domain



Choose domains to display within the console

3. Choose your domain from the list.

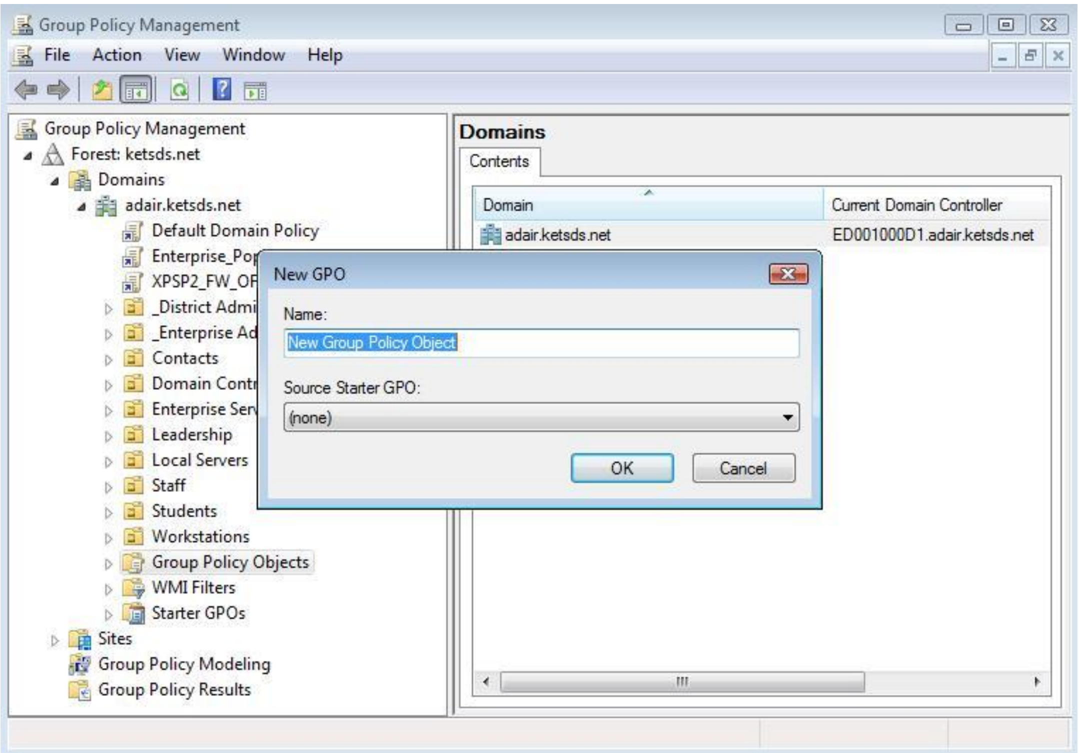
4. Expand “Domains” and then domain name



Domain	Current Domain Controller
adair.ketsds.net	ED001000D1.adair.ketsds.net

1. **Right click on "GROUP POLICY OBJECTS" then click "NEW"**

2. **Give your new GPO a name and select a "Source Starter GPO"* if applicable.**
   ***A source starter GPO is a template GPO to start with.**

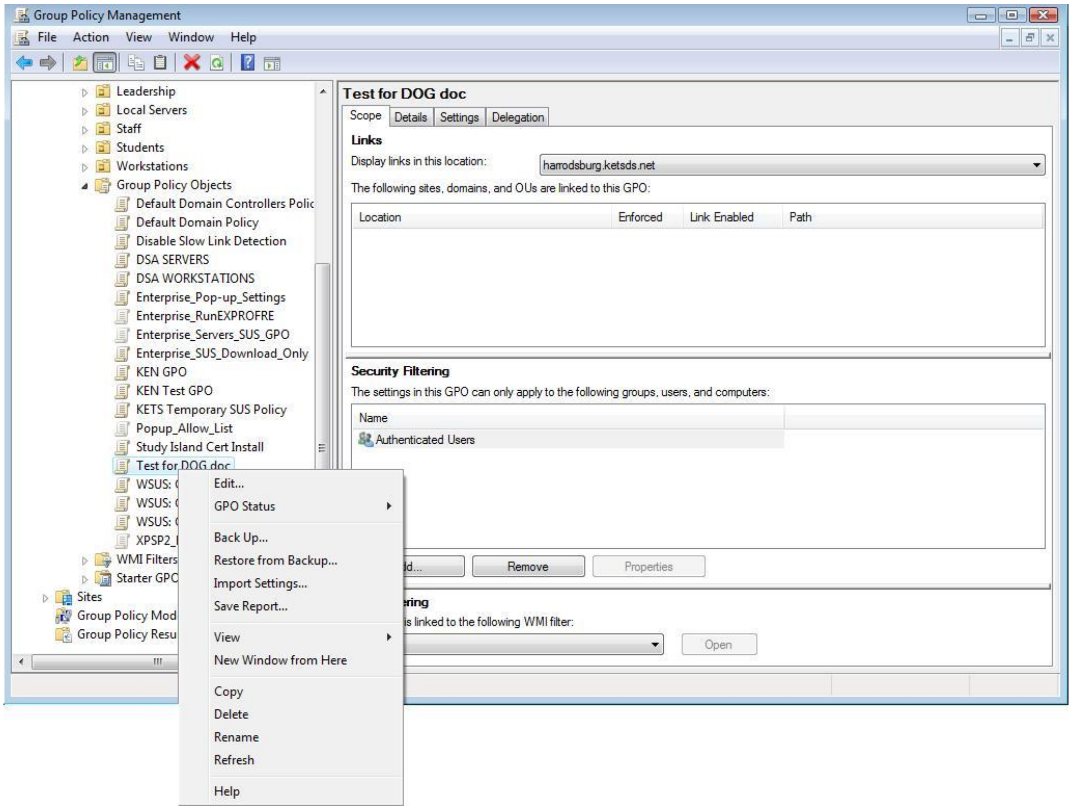


Domain	Current Domain Controller
adair.ketsds.net	ED001000D1.adair.ketsds.net

Name: New Group Policy Object

Source Starter GPO: (none)

3. **Right click on the name of the GPO you just created and click edit.**



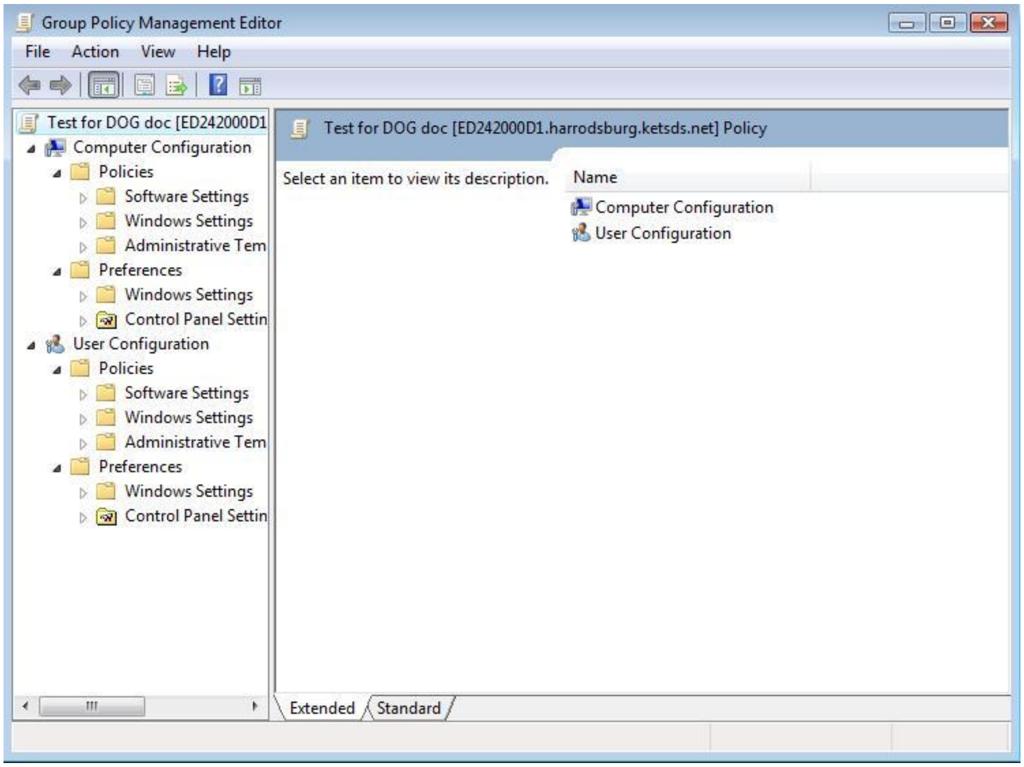
Display links in this location: harrodsburg.ketsds.net

The following sites, domains, and OUs are linked to this GPO:

The settings in this GPO can only apply to the following groups, users, and computers:

is linked to the following WMI filter:

4. **Set your policies and preferences in the Group Policy Management Editor.**

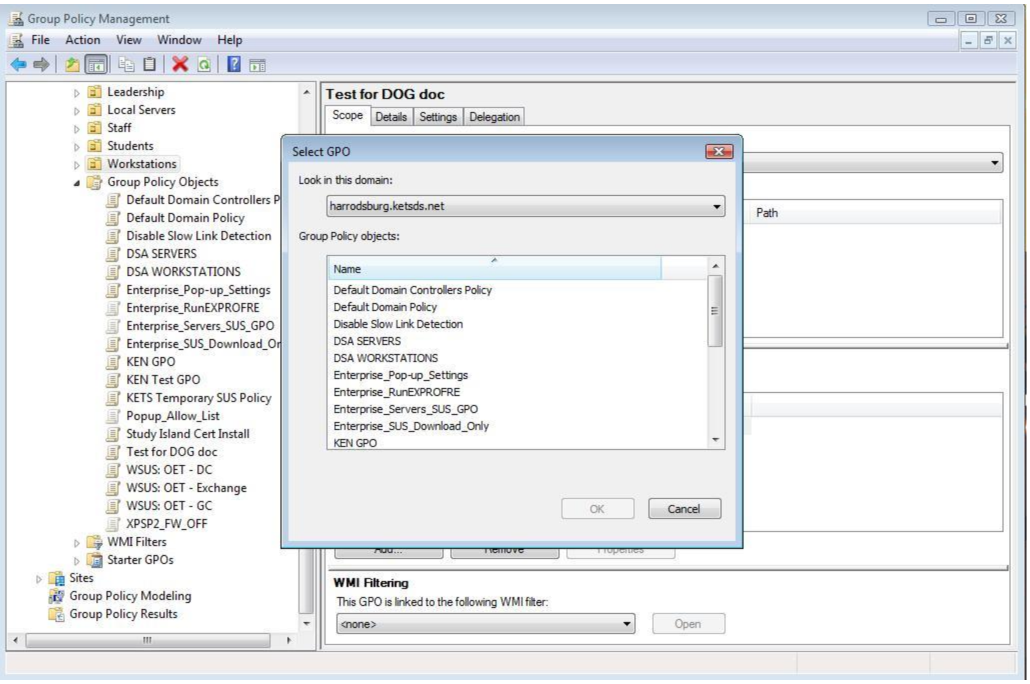


Select an item to view its description.

5. **Click file exit to close Group Policy Management Editor.**

6. **Right click on the OU you wish to link your new group policy to and click "LINK an EXSISTING GPO"**

7. **Highlight the GPO you wish to link from the list of Group Policy objects and click "OK".**



Test for DOG doc

Select GPO

Look in this domain: harrodsburg.ketsds.net

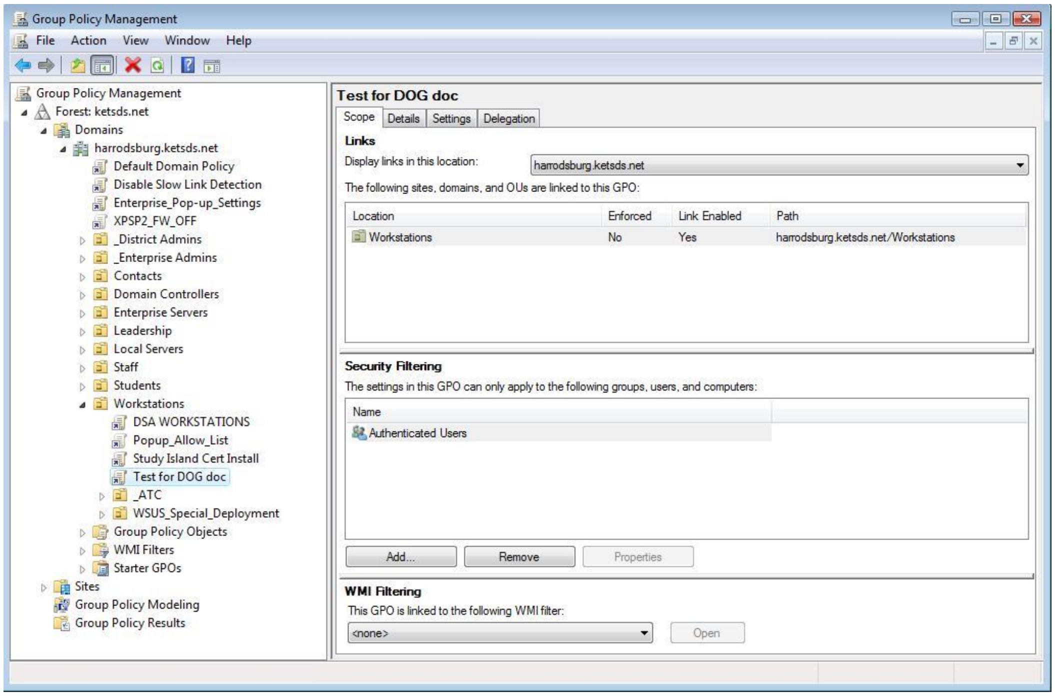
Group Policy objects:

Name
Default Domain Controllers Policy
Default Domain Policy
Disable Slow Link Detection
DSA SERVERS
DSA WORKSTATIONS
Enterprise_Pop-up_Settings
Enterprise_RunEXPROFRE
Enterprise_Servers_SUS_GPO
Enterprise_SUS_Download_Only
KEN GPO

WMI Filtering

This GPO is linked to the following WMI filter: <none>

8. **Expand the OU you just linked your Group Policy to and verify it is there and enabled.**



Test for DOG doc

Links

Display links in this location: harrodsburg.ketsds.net

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
Workstations	No	Yes	harrodsburg.ketsds.net/Workstations

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter: <none>

The GPO will be applied the next time the Computer Policy is applied to a workstation/server in this OU. The Computer Policy will be applied after the next reboot. If you would like to apply the policy without a reboot, the command GPUPDATE /FORCE can be supplied at a command prompt.

2. Group Policy to remotely install software

Create a Distribution Point

1. Log on to the server computer using an account in the **Group Policy Creator Owners** group.
2. Create a shared network folder where you will put the Microsoft Windows Installer package (.msi file) that you want to distribute.
3. Set permissions on the share to allow access to the distribution package.
4. Copy or install the package to the distribution point. For example, to distribute Microsoft Office XP, run the administrative installation (setup.exe /a) to copy the files to the distribution point.

Create a Group Policy Object

1. Start the Active Directory Users and Computers snap-in. To do this, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, right-click your domain, and then click **Properties**.
3. Click the **Group Policy** tab, and then click **New**.
4. Type a name for this new policy (for example, Office XP distribution), and then press ENTER.
5. Click **Properties**, and then click the **Security** tab.
6. Click to clear the **Apply Group Policy** check box for the security groups that you want to prevent from having this policy applied.
7. Click to select the **Apply Group Policy** check box for the groups that you want this policy to apply to.
8. When you are finished, click **OK**.

Assign a Package

1. Start the Active Directory Users and Computers snap-in. To do this, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, right-click your domain, and then click **Properties**.
3. Click the **Group Policy** tab, select the group policy object that you want, and then click **Edit**.
4. Under **Computer Configuration**, expand **Software Settings**.
5. Right-click **Software installation**, point to **New**, and then click **Package**.
6. In the **Open** dialog box, type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example, \\*file server**share**file name*.msi.

   Important Do not use the **Browse** button to access the location. Make sure that you use the UNC path to the shared installer package.
7. Click **Open**.
8. Click **Assigned**, and then click **OK**. The package is listed in the right pane of the **Group Policy** window.
9. Close the **Group Policy** snap-in, click **OK**, and then quit the Active Directory Users and Computers snap-in.

10. When the client computer starts, the managed software package is automatically installed.

Remove Programs tool in **Control Panel**:

1. Start the Active Directory Users and Computers snap-in. To do this, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, right-click your domain, and then click **Properties**.
3. Click the **Group Policy** tab, click the group policy object that you want, and then click **Edit**.
4. Under **User Configuration**, expand **Software Settings**.
5. Right-click **Software installation**, point to **New**, and then click **Package**.
6. In the **Open** dialog box, type the full UNC path of the shared installer package that you want. For example, \\*file server**share***file name**.msi.

   Important Do not use the **Browse** button to access the location. Make sure that you use the UNC path to the shared installer package.
7. Click **Open**.
8. Click **Publish**, and then click **OK**.
9. The package is listed in the right pane of the **Group Policy** window.
10. Close the Group Policy snap-in, click **OK**, and then quit the Active Directory Users and Computers snap-in.
11. Test the package:

    Note Because there are several versions of Microsoft Windows, the following steps may be different on your computer. If they are, see your product documentation to complete these steps.
    a. Log on to a workstation that is running Windows 2000 Professional or Windows XP Professional by using an account that you published the package to.
    b. In Windows XP, click **Start**, and then click **Control Panel**.
    c. Double-click **Add or Remove Programs**, and then click **Add New Programs**.
    d. In the **Add programs from your network** list, click the program that you published, and then click **Add**. The program is installed.
    e. Click **OK**, and then click **Close**.

Redeploy a Package

1. Start the Active Directory Users and Computers snap-in. To do this, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, right-click your domain, and then click **Properties**.
3. Click the **Group Policy** tab, click the Group Policy object that you used to deploy the package, and then click **Edit**.
4. Expand the **Software Settings** container that contains the software installation item that you used to deploy the package.
5. Click the software installation container that contains the package.
6. In the right pane of the **Group Policy** window, right-click the program, point to **All Tasks**, and then click **Redeploy application**. You will receive the following message:

Redeploying this application will reinstall the application everywhere it is already installed. Do you want to continue?

7. Click **Yes**.
8. Quit the Group Policy snap-in, click **OK**, and then quit the Active Directory Users and Computers snap-in.

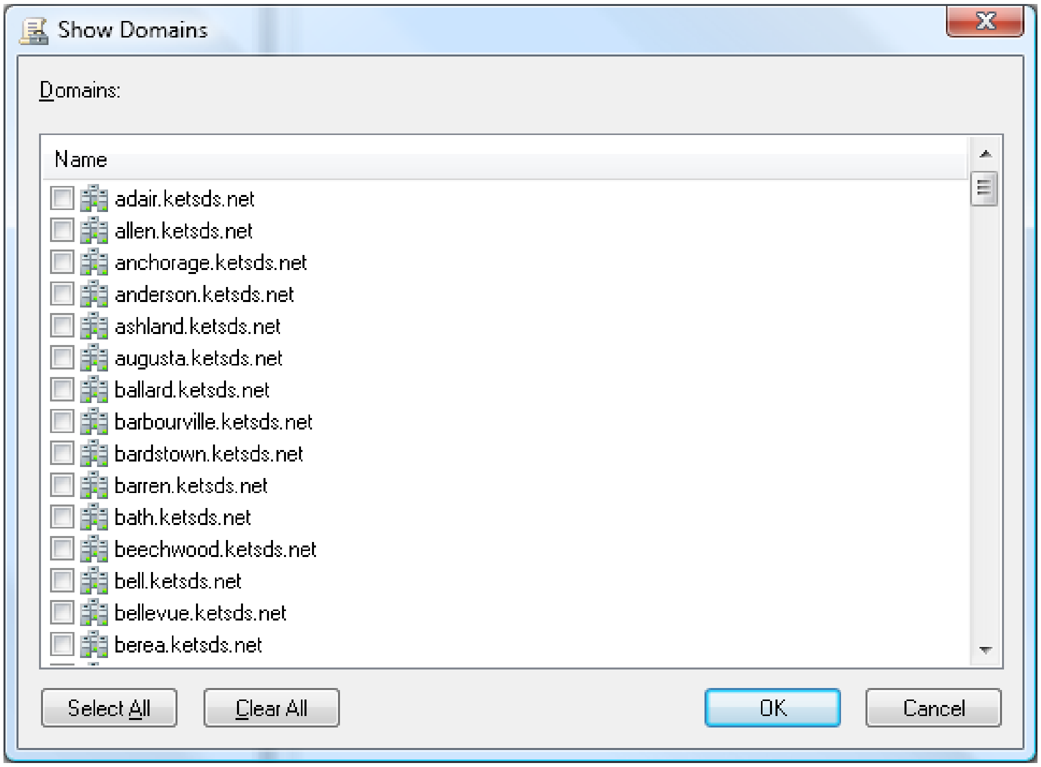
Remove a Package

1. Start the Active Directory Users and Computers snap-in. To do this, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, right-click your domain, and then click **Properties**.
3. Click the **Group Policy** tab, click the Group Policy object that you used to deploy the package, and then click **Edit**.
4. Expand the **Software Settings** container that contains the software installation item that you used to deploy the package.
5. Click the software installation container that contains the package.
6. In the right pane of the **Group Policy** window, right-click the program, point to **All Tasks**, and then click **Remove**.
7. Do one of the following:
   - Click **Immediately uninstall the software from users and computers**, and then click **OK**.
   - Click **Allow users to continue to use the software but prevent new installations,** and then click **OK**.
8. Quit the Group Policy snap-in, click **OK**, and then quit the Active Directory Users and Computers snap-in.

3. Group Policy to remotely install Certificates

PREREQUISITES: The certificate should be in a shared network location that all users have read access.

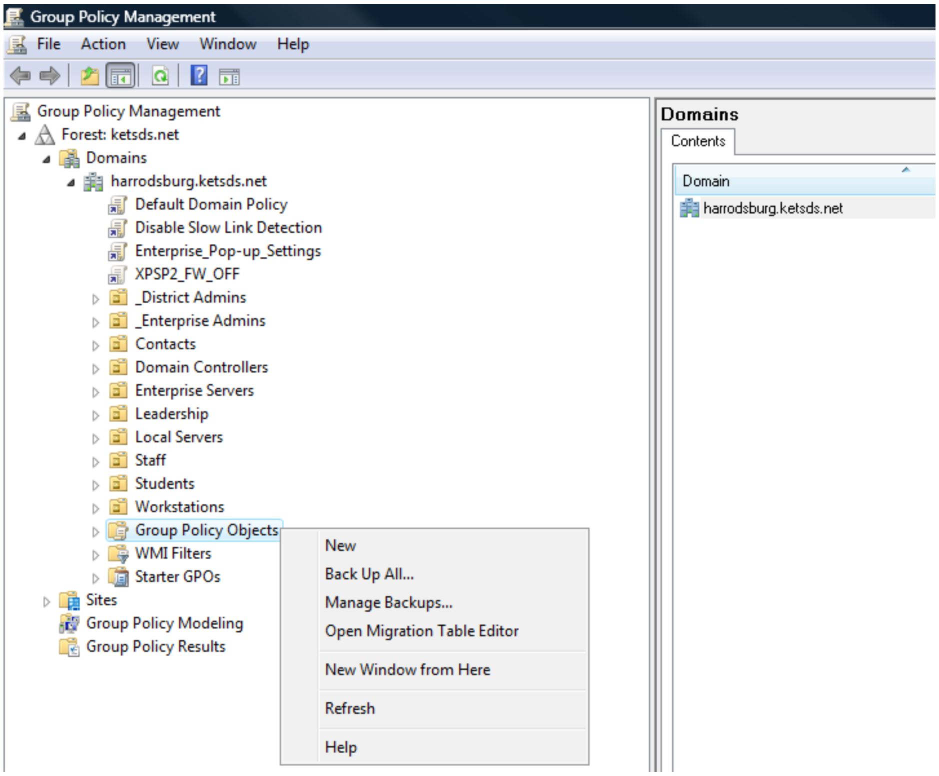
1. Open the Group Policy Management Console
2. Right click ***DOMAINS***, and choose ***SHOW DOMAINS***
3. Select your domain by placing a checkmark in the box and click ***OK***


Show Domains

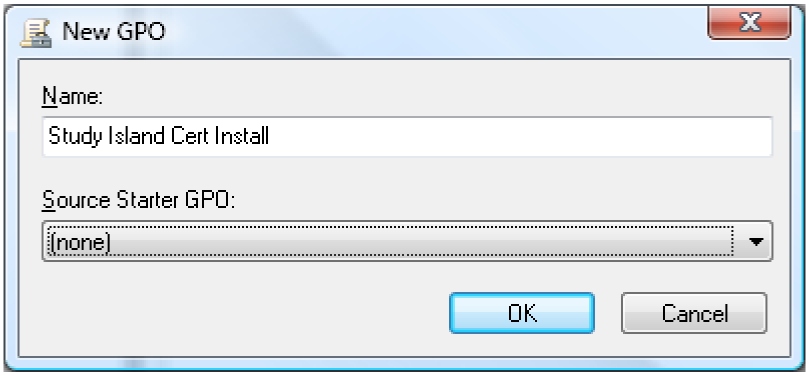
Domains:

Name
□ adair.ketsds.net
□ allen.ketsds.net
□ anchorage.ketsds.net
□ anderson.ketsds.net
□ ashland.ketsds.net
□ augusta.ketsds.net
□ ballard.ketsds.net
□ barbourville.ketsds.net
□ bardstown.ketsds.net
□ barren.ketsds.net
□ bath.ketsds.net
□ beechwood.ketsds.net
□ bell.ketsds.net
□ bellevue.ketsds.net
□ berea.ketsds.net

4. Right click ***GROUP POLICY OBJECTS*** in the left pane and select ***NEW***



5. Name the policy using a name that explains what the policy will do. Leave the Source Starter GPO field at the default and click ***OK***.



New GPO

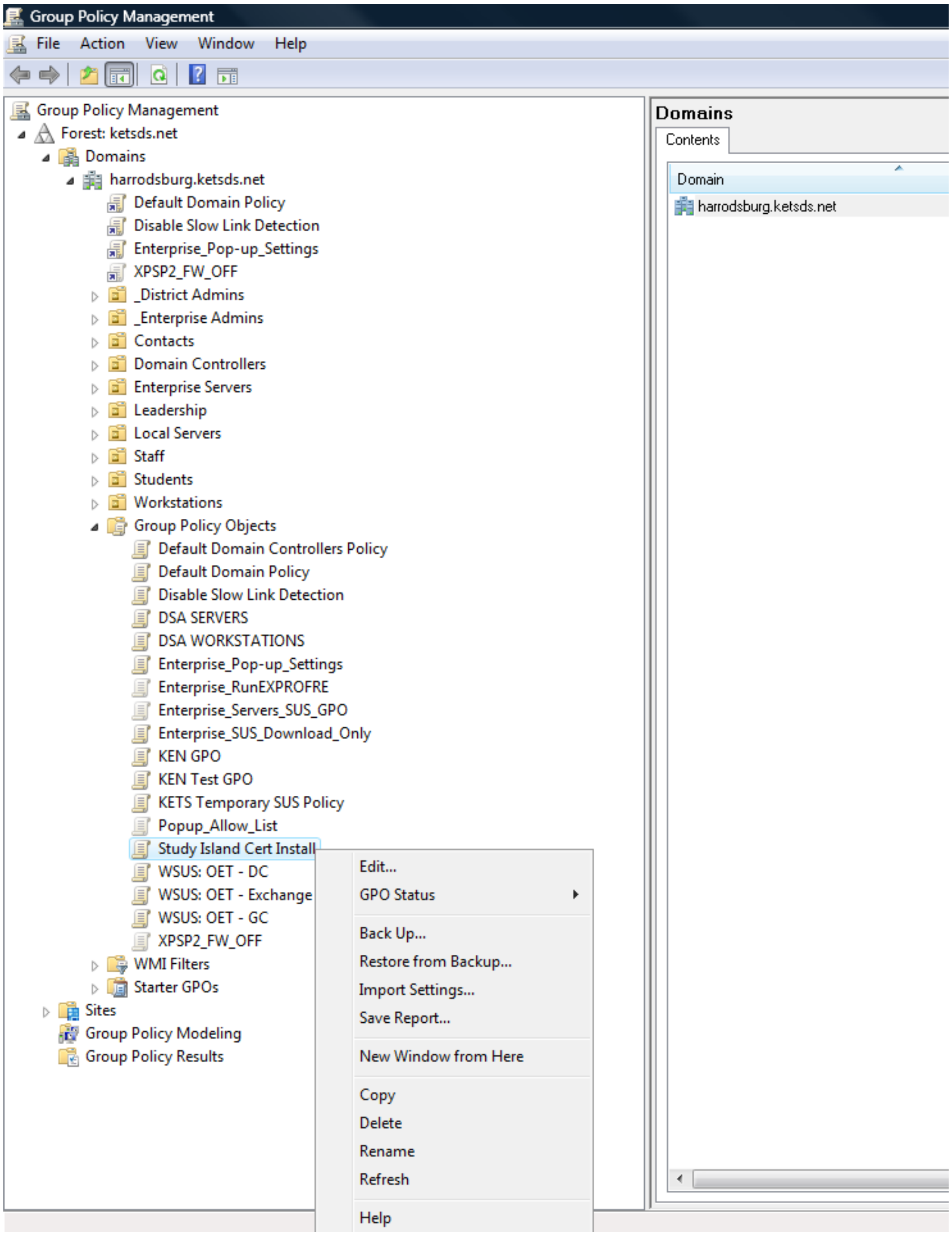
Name:

Study Island Cert Install

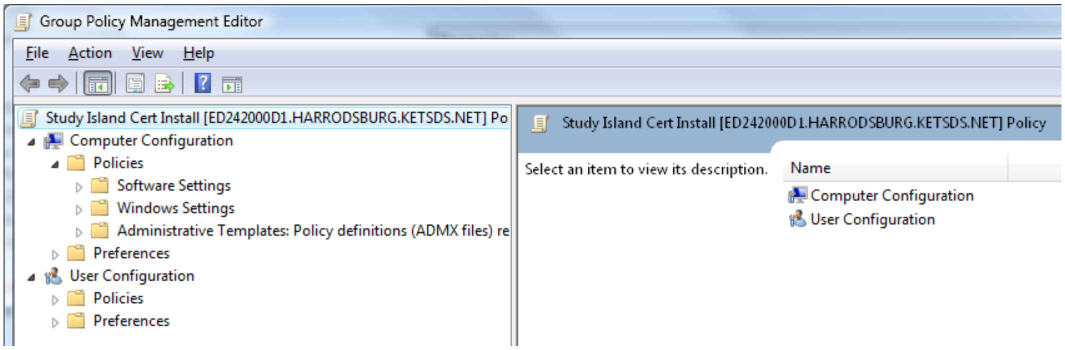
Source Starter GPO:

(none)

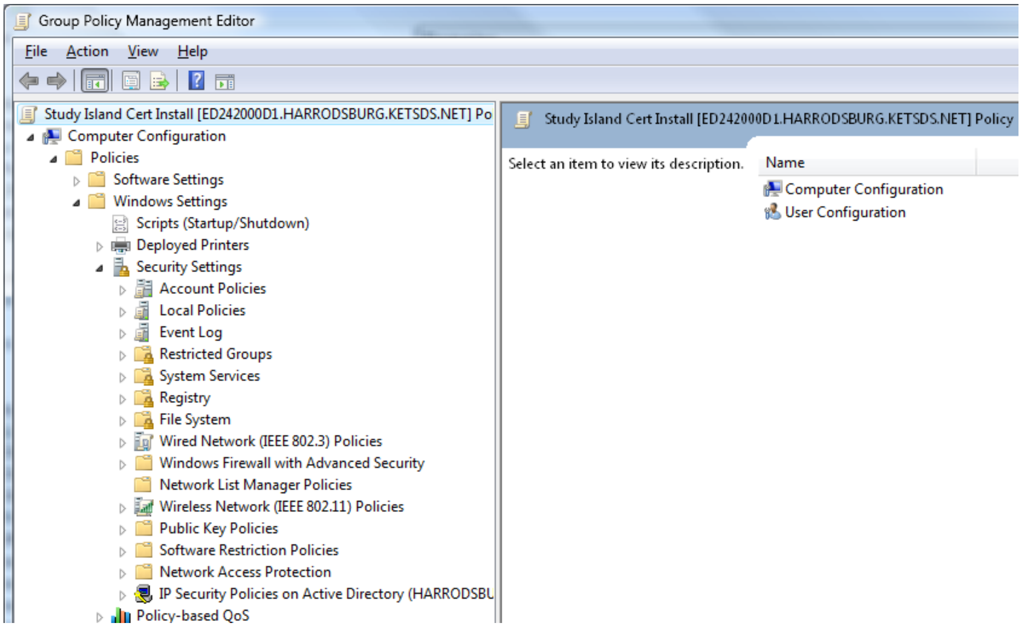
6. Expand ***GROUP POLICY OBJECTS*** in the left pane and right click the new policy you created in step 5. Select ***EDIT…***



7. Expand ***COMPUTER CONFIGURATION***, then ***POLICIES***


Group Policy Management Editor
File Action View Help
Study Island Cert Install [ED242000D1.HARRODSBURG.KETSDS.NET] Po
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy definitions (ADMX files) re
Preferences
User Configuration
Policies
Preferences
Study Island Cert Install [ED242000D1.HARRODSBURG.KETSDS.NET] Policy
Select an item to view its description.
Name
Computer Configuration
User Configuration

8. Expand ***WINDOWS SETTINGS***, then ***SECURITY SETTINGS***



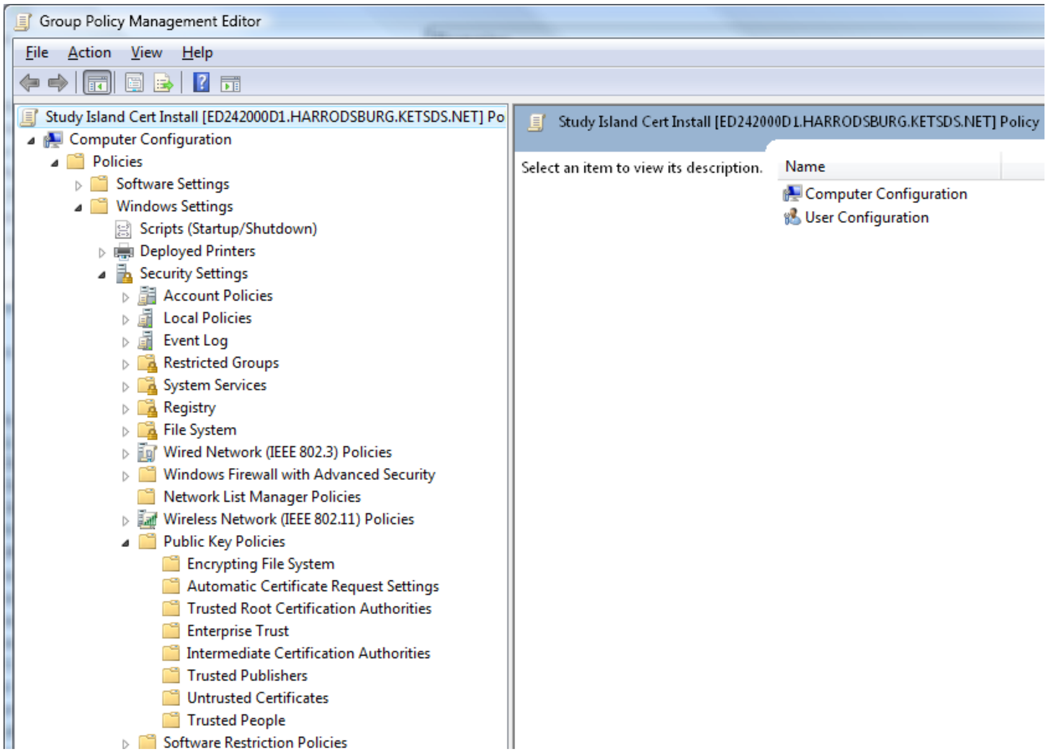
- Study Island Cert Install [ED242000D1.HARRODSBURG.KETSDS.NET] Po
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Scripts (Startup/Shutdown)
        - Deployed Printers
        - Security Settings
          - Account Policies
          - Local Policies
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Policies
          - Windows Firewall with Advanced Security
          - Network List Manager Policies
          - Wireless Network (IEEE 802.11) Policies
          - Public Key Policies
          - Software Restriction Policies
          - Network Access Protection
          - IP Security Policies on Active Directory (HARRODSBU
        - Policy-based QoS

Study Island Cert Install [ED242000D1.HARRODSBURG.KETSDS.NET] Policy

Select an item to view its description.

Name
Computer Configuration
User Configuration

9. Expand PUBLIC KEY POLICIES



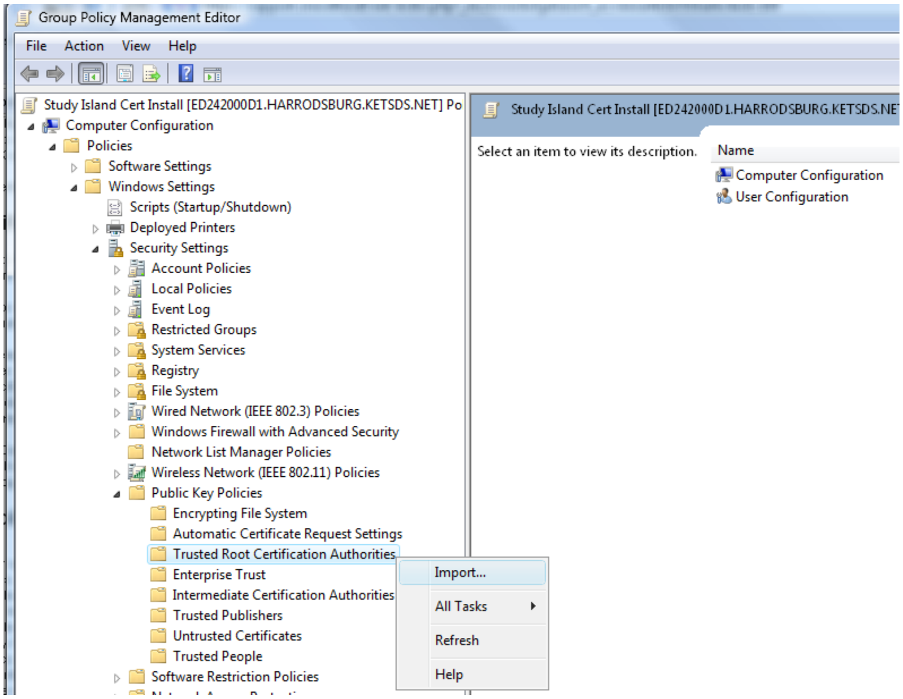
- Study Island Cert Install [ED242000D1.HARRODSBURG.KETSDS.NET] Po
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Scripts (Startup/Shutdown)
        - Deployed Printers
        - Security Settings
          - Account Policies
          - Local Policies
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Policies
          - Windows Firewall with Advanced Security
          - Network List Manager Policies
          - Wireless Network (IEEE 802.11) Policies
          - Public Key Policies
            - Encrypting File System
            - Automatic Certificate Request Settings
            - Trusted Root Certification Authorities
            - Enterprise Trust
            - Intermediate Certification Authorities
            - Trusted Publishers
            - Untrusted Certificates
            - Trusted People
          - Software Restriction Policies

Study Island Cert Install [ED242000D1.HARRODSBURG.KETSDS.NET] Policy

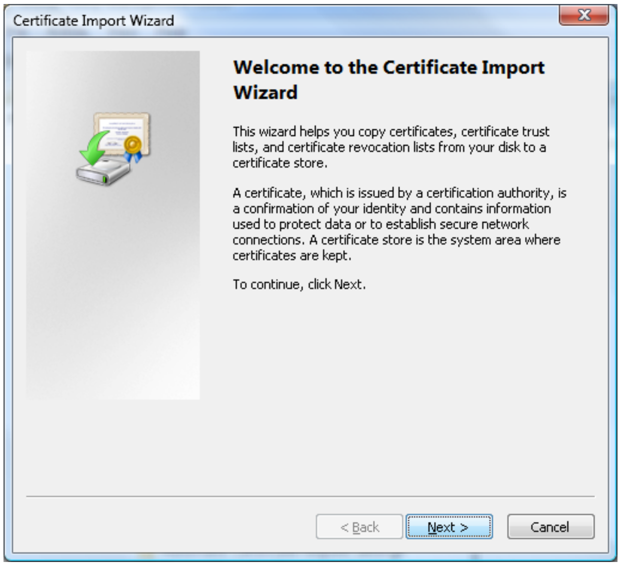
Select an item to view its description.

Name
Computer Configuration
User Configuration

10. Right click ***TRUSTED ROOT CERTIFICATION AUTHORITIES*** and select ***IMPORT***


Group Policy Management Editor
File Action View Help
Study Island Cert Install [ED242000D1.HARRODSBURG.KETSDS.NET] Po
Computer Configuration
Policies
Software Settings
Windows Settings
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Software Restriction Policies
Import...
All Tasks
Refresh
Help
Study Island Cert Install [ED242000D1.HARRODSBURG.KETSDS.NE
Select an item to view its description.
Name
Computer Configuration
User Configuration

11. When the Certificate Import Wizard appears, click ***NEXT***



Certificate Import Wizard

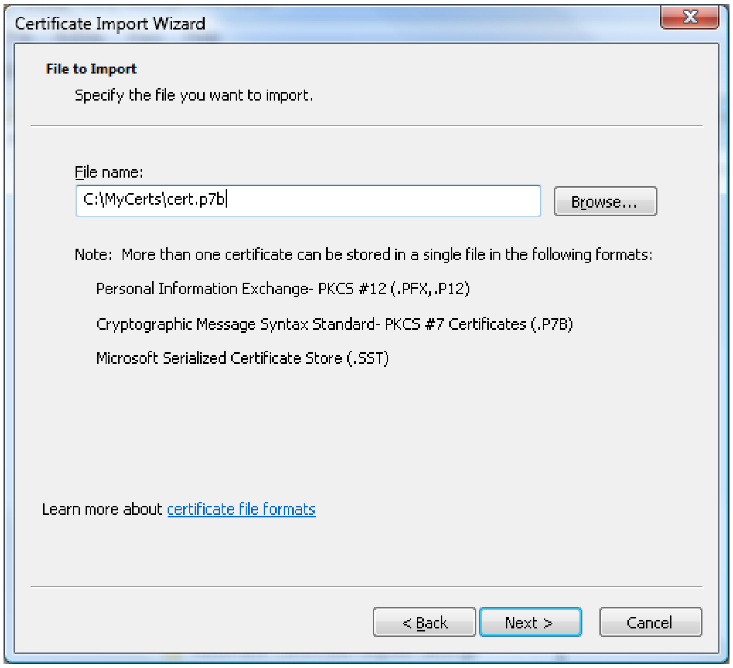
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

12. Browse to the location of the certificate and click NEXT



File to Import

Specify the file you want to import.

File name:

C:\MyCerts\cert.p7b

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

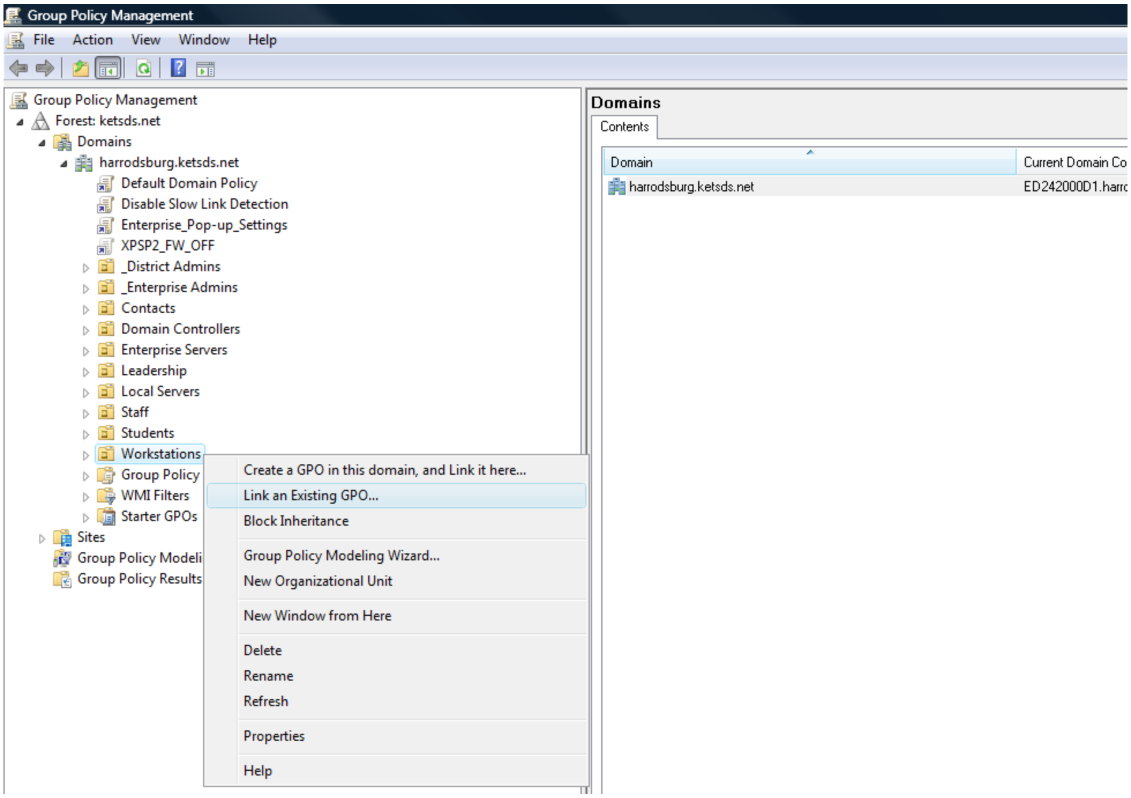
Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

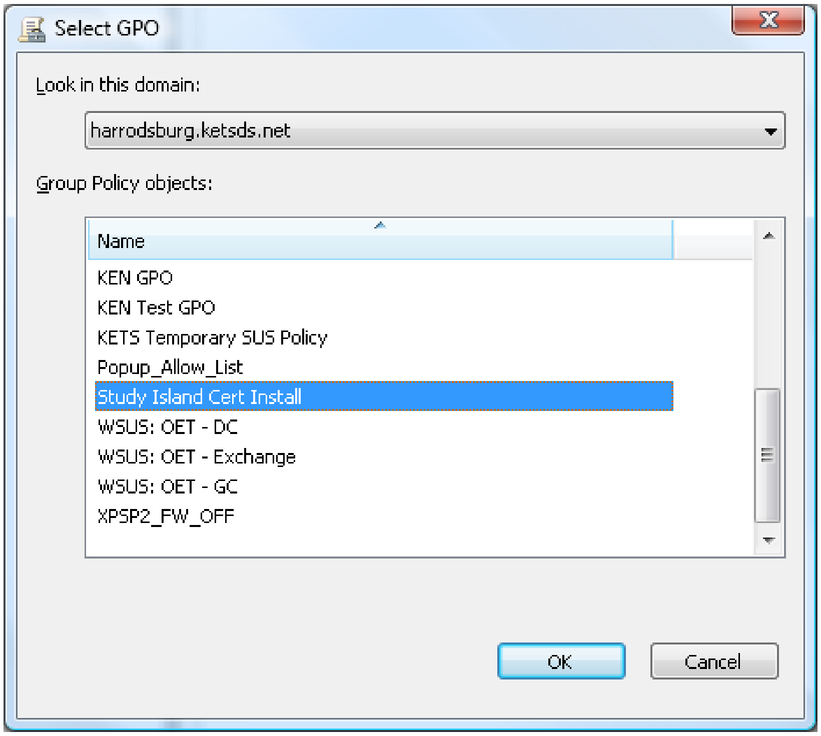
13. Accept the remaining defaults and click finish on the final dialog.

14. Close the Group Policy Management Editor Window

15. Right click the OU that contains the workstations to which this policy needs to be applied and select ***LINK AN EXISTING GPO…***



16. Verify that your domain is selected in the ***LOOK IN THIS DOMAIN*** field and select the policy that you created in Step 5.


Select GPO

Look in this domain:

harrodsburg.ketsds.net

Group Policy objects:

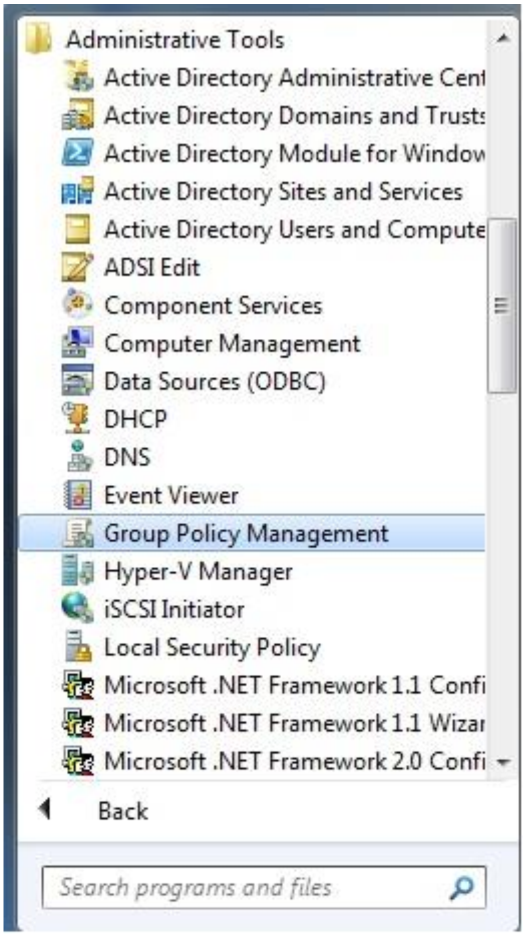
Name
KEN GPO
KEN Test GPO
KETS Temporary SUS Policy
Popup_Allow_List
Study Island Cert Install
WSUS: OET - DC
WSUS: OET - Exchange
WSUS: OET - GC
XPSP2_FW_OFF

17. Click OK

The certificate will be installed the next time the Computer Policy is applied to a workstation in this OU. The Computer Policy will be applied after the next reboot. If you would like to apply the policy without a reboot, the command GPUPDATE /FORCE can be supplied at a command prompt.

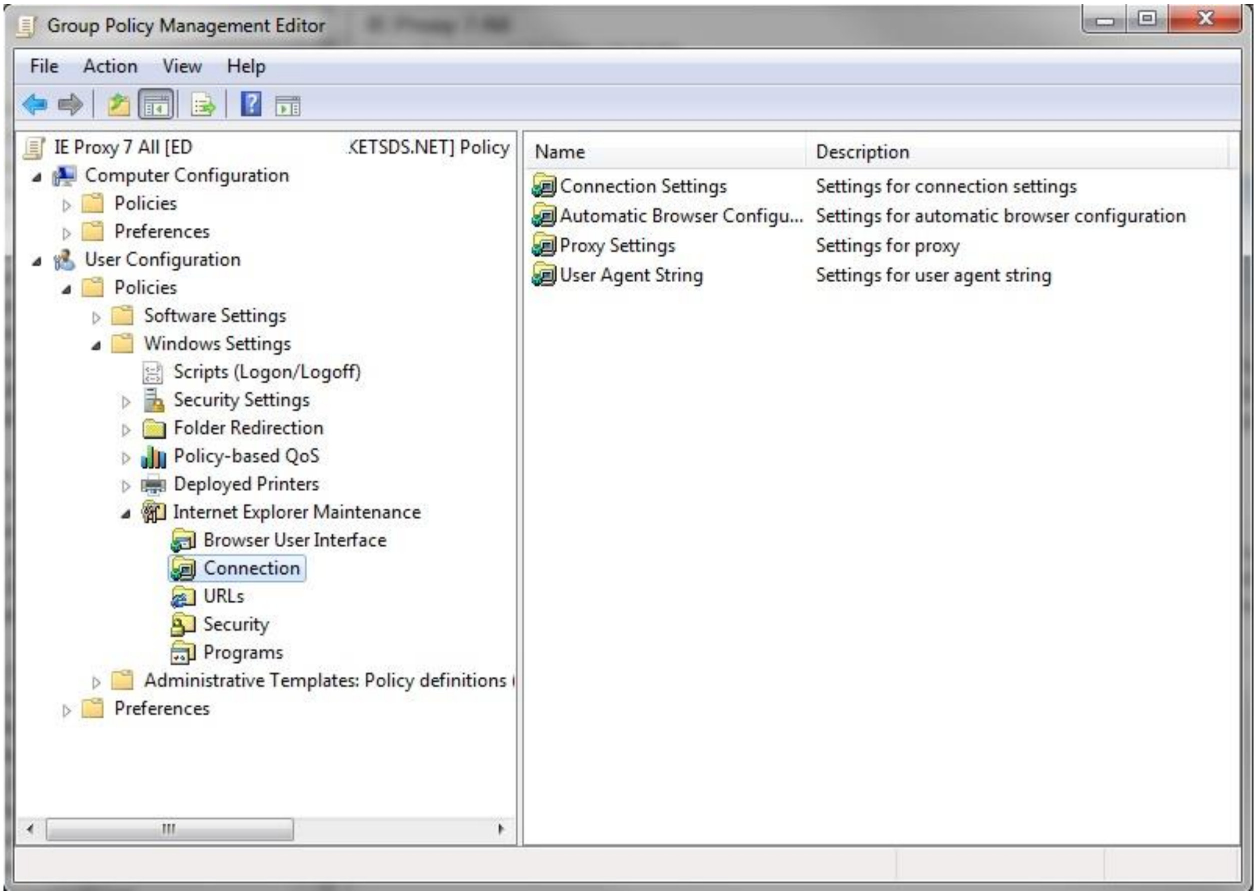
4. Group Policy to Configure Proxy Settings in Internet Explorer

1. Open the **Group Policy Management Console (GPMC)**


Administrative Tools
Active Directory Administrative Cent
Active Directory Domains and Trusts
Active Directory Module for Window
Active Directory Sites and Services
Active Directory Users and Compute
ADSI Edit
Component Services
Computer Management
Data Sources (ODBC)
DHCP
DNS
Event Viewer
Group Policy Management
Hyper-V Manager
iSCSI Initiator
Local Security Policy
Microsoft .NET Framework 1.1 Confi
Microsoft .NET Framework 1.1 Wizar
Microsoft .NET Framework 2.0 Confi
Back
Search programs and files

2. Create a new group policy

3. Browse to **User Configuration -> Windows Settings -> Internet Explorer Maintenance -> Connection**

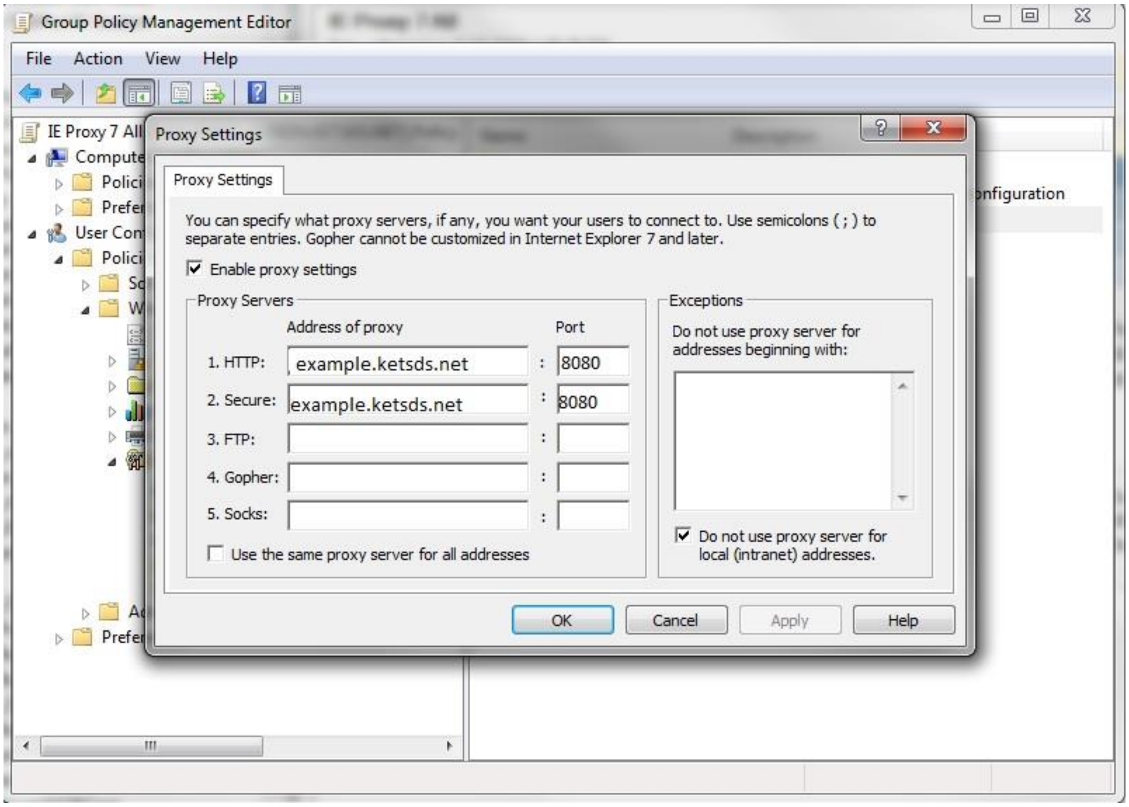


IE Proxy 7 All [ED KETSDS.NET] Policy

- Computer Configuration
  - Policies
  - Preferences
- User Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Scripts (Logon/Logoff)
      - Security Settings
      - Folder Redirection
      - Policy-based QoS
      - Deployed Printers
      - Internet Explorer Maintenance
        - Browser User Interface
        - Connection
        - URLs
        - Security
        - Programs
    - Administrative Templates: Policy definitions (
  - Preferences

Name	Description
Connection Settings	Settings for connection settings
Automatic Browser Configu...	Settings for automatic browser configuration
Proxy Settings	Settings for proxy
User Agent String	Settings for user agent string

4. Double click **PROXY SETTINGS** to open the configuration window



Proxy Settings

You can specify what proxy servers, if any, you want your users to connect to. Use semicolons (;) to separate entries. Gopher cannot be customized in Internet Explorer 7 and later.

☑ Enable proxy settings

Proxy Servers

	Address of proxy		Port
1. HTTP:	example.ketsds.net	:	8080
2. Secure:	example.ketsds.net	:	8080
3. FTP:		:	
4. Gopher:		:	
5. Socks:		:	

□ Use the same proxy server for all addresses

Exceptions

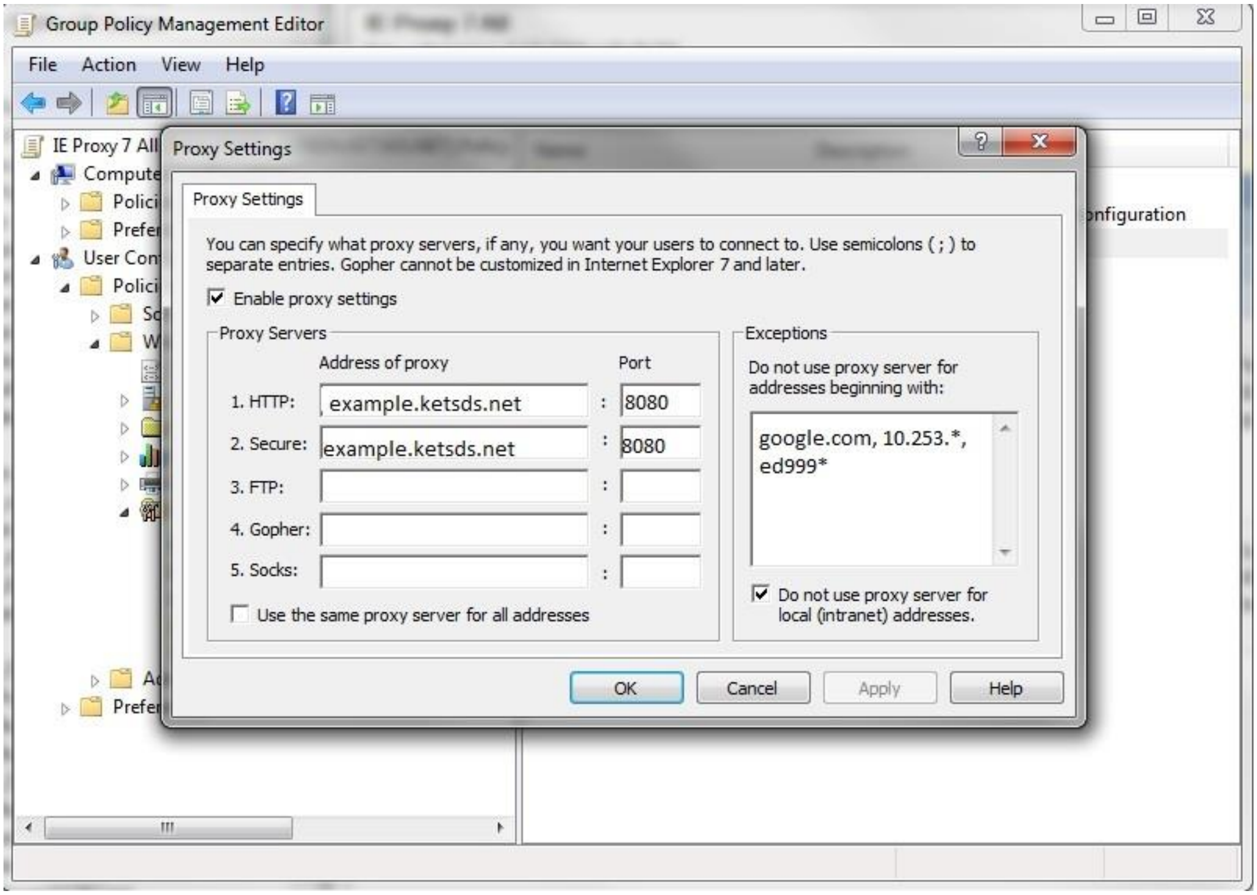
Do not use proxy server for addresses beginning with:

☑ Do not use proxy server for local (intranet) addresses.

5. Check **ENABLE PROXY SETTINGS**

6. Input proxy server FQDN or IP address and port.

7. Add exceptions for sites and servers you wish to **BYPASS** proxy settings.



Proxy Settings

Proxy Settings

You can specify what proxy servers, if any, you want your users to connect to. Use semicolons (;) to separate entries. Gopher cannot be customized in Internet Explorer 7 and later.

☑ Enable proxy settings

Proxy Servers

	Address of proxy		Port
1. HTTP:	example.ketsds.net	:	8080
2. Secure:	example.ketsds.net	:	8080
3. FTP:		:	
4. Gopher:		:	
5. Socks:		:	

☐ Use the same proxy server for all addresses

Exceptions

Do not use proxy server for addresses beginning with:

google.com, 10.253.*, ed999*

☑ Do not use proxy server for local (intranet) addresses.

8. The Computer Policy will be applied after the next reboot. If you would like to apply the policy without a reboot, the command **GPUPDATE /FORCE** can be supplied at a command prompt.